対称3進算術AN符号に関する研究

昭和61年3月

大倉良昭

対称３進算術ＡＮ符号に関する研究

昭 和 61 年 3 月

大　倉　良　昭

目　次

第１章　緒　論 …… 1

１．１　本研究の背景と目的 …… 1

１．２　概　要 …… 3

第２章　対称３進算術重みと対称３進算術距離 …… 6

２．１　緒　言 …… 6

２．２　整数の対称３進表現と誤りの値 …… 6

２．３　算術重みと算術距離 …… 8

２．４　整数の３進表現と算術重み …… 10

２．５　モジュラ重みとモジュラ距離 …… 11

２．６　結　言 …… 13

第３章　ＳＴ－ＡＮ符号 …… １８

３．１　緒　言 …… 18

３．２　ＳＴ－ＡＮ符号 …… 18

３．３　最小距離と誤り訂正能力 …… 19

３．４　最小距離と情報整数の範囲 …… 20

３．４．１　最小距離2の符号（$M_{ST}(A,2)$） …… 21

３．４．２　最小距離3の符号（$M_{ST}(A,3)$） …… 21

３．４．３　最小距離4の符号（$M_{ST}(A,4)$） …… 25

３．５　結　言 …… 31

第４章　巡回ＳＴ－ＡＮ符号 …… ３７

４．１　緒　言 …… 37

４．２　巡回ＳＴ－ＡＮ符号の構造 …… 37

４．３　最小距離と誤り訂正能力 …… 40

４．４　素符号の重み …… 42

第５章　巡回ＳＴ－ＡＮ符号の最小距離 …… ４４
５．１　緒　言 …… 44
５．２　最小距離の算定 …… 44
５．３　符号語数Ｂ＝ｐ，２ｐ，４ｐの場合 …… 45
５．４　符号語数Ｂ＝p^{α}，$2p^{\alpha}$，$4p^{\alpha}$ の場合 …… 54
５．５　符号語数Ｂ＝2^{γ} の場合 …… 67
５．６　符号語数Ｂ＝ｐｑ，２ｐｑの場合 …… 70
５．７　符号語数Ｂ＝$p^{\alpha}q$，$2p^{\alpha}q$の場合 …… 79
５．８　符号語数Ｂ＝$p^{\alpha}q^{\beta}$，$2p^{\alpha}q^{\beta}$ の場合 …… 94
５．９　最小距離算定結果のまとめ …… 106
５．10　結　言 …… 107
５-Ａ　付　録；補題の証明 …… 110

第６章　負巡回ＳＴ－ＡＮ符号 …… １１６
６．１　緒　言 …… 116
６．２　負巡回シフトと負巡回ＳＴ－ＡＮ符号の定義 …… 116
６．３　巡回ＳＴ－ＡＮ符号との関係 …… 121
６．４　負巡回ＳＴ－ＡＮ符号の最小距離 …… 122
６．５　結　言 …… 124

第７章　ＳＴ－ＡＮ符号の復号 …… １２７
７．１　緒　言 …… 127
７．２　ＳＴ－ＡＮ符号の一般的な復号 …… 127
７．３　巡回ＳＴ－ＡＮ符号の復号 …… 130
７．３．１　単純エラー・トラッピング …… 130
７．３．２　窓付きエラー・トラッピング …… 134
７．３．３　検査窓の配置 …… 138
７．４　負巡回ＳＴ－ＡＮ符号の復号 …… 142

７．５　多数決論理復号可能な巡回ＳＴ－ＡＮ符号の復号 … 146
７．５．１　１段多数決論理復号 …… 147
７．５．２　２段多数決論理復号 …… 150
７．５．３　ｋ段多数決論理復号 …… 152
７．６　結　言 …… 156

第８章　結　論 …… １６５

謝　辞 …… 167

参考文献 …… 168

第1章　緒　論

1．1　本研究の背景と目的

最近のディジタルデータ通信システムにおいては，通信量の増大と通信速度の向上が著しく，それらの通信内容や通信方式はますます多様化の一途をたどっている．このため，これらの端末に電子計算機やそれに匹敵する複雑なディジタルデータ処理装置が導入されている．また，電子計算機システムにおいては，稼働効率の向上，ハードウェアやソフトウェア等の資源の有効利用のための計算機ネットワーク化が盛んに行われている．将来，このような傾向は更に高まり，十分な信頼性を確保すると共に，データ伝送および演算などのデータ処理装置の高速化と高能率化が一層厳しく要求される．これらの要求を満たすことができる方法の一つとして，システムの多値化が考えられる．多値論理回路に関する研究も盛んに行われているが，実用化に耐えうる安定な多値論理素子の開発が遅れている現在，２値素子による多値論理基本回路の構成方式が採られている[25][28]．新素子の開発や集積化技術などのハードウェアの進歩に伴い，多値システム実現の可能性は高い．

多値ディジタルシステムにおける信頼性の要求に対しては，算術ＡＮ符号が考えられる．算術ＡＮ符号は，演算実行途中に生じる誤りも伝送途中に生じる誤りと同様にして検出訂正が可能な符号であり，J.M.Diamond[9]やD.T.Brown[3]により，提案されて以来，数多く研究され，２進の場合においては相当の成果が報告されている[12][36][39]．これらを拡張した非２進算術ＡＮ符号については，T.R.N.RaoとA.K.Trehan[37]，その他の研究[10][12][30]もあるが，本論文は３進表現独特の対称３進算術ＡＮ符号を提案するものである．

３進数の各けたの数字に {0,1,2} を用いる表現と {-1,0,1} を用いる表現がある．前者は通常の３進表現であり，後者は特に対称３進表現あるいはST表現[29]と呼ばれている．対称３進表現は，正負両数を統一的に処理するのに適した数表現であり，算術演算処理を簡明で能率的なものにする３進独特のものである[26]．

このような特長を生かした種々の３値ディジタルシステムがすでに開発されている[8][19][27][42]．しかしながら，このような対称３進表現に基づく３値ディジタルシステムの信頼性を向上させるための３進算術ＡＮ符号に関する研究はこれまでなされなかったようである．

算術ＡＮ符号は整数Nに一定の整数Aを乗算したものANの集合として定義される．符号化すべき整数Nは情報整数，定数Aは生成数という．このような符号は線形な符号であり，一般には非組織的な非分離型符号である．先のDiamondやBrownは，電子計算機の演算装置における基本演算である加減算の誤り検出，訂正を目的として，この符号を提案し，具体的な２進符号の例を挙げている．以後，算術ＡＮ符号は，応用的あるいは理論的見地から研究され，１９６０年代より急速に発展してきた．これは，以下の理由によるものと考えられる．

(1) 算術演算装置や記憶装置およびディジタルデータ伝送路で生じる誤りの検出訂正に有効である[36]．

(2) 符号化，復号に伴う処理が算術的であって，これらの処理を実行するための特別な装置を必要としない[7]．

(3) 代数的線形符号に対照される類似の性質や構造をもち，これらと並行した理論展開ができる[4][13][24]．

(4) 整数論[43]で得られている結果を符号の具体的な構成，誤り訂正能力の算定に利用できる．

W.W.Peterson[36]やD.Mandelbaum[23]により提案された巡回算術ＡＮ符号は，法$2^n-1=AB$に関する整数の剰余環におけるAの倍数からなるイディアールであって，巡回けた移動の操作のもとに閉じており，加算のみならず電子計算機の演算装置で実行されるその他の演算における誤りに対しても有効である．さらに，T.R.N. Rao とO.N.Garcia[38]は，整数の法$2^n-1=AB$に関する剰余環上での距離測度を導入して，負数の表現に伴う補数処理にも有効であることを示した．さらに，半導体集積化技術の進歩に伴って，P.G.NeumannとRao[30]は，バイト単位の集積回路で構成される演算装置の高信頼化を目的とした2^e進符号を提案した．このような巡回算術ＡＮ符号に関する研究は電子計算機の演算装置への応用に大きく貢献するものである．また，主として(3)の理由から代数的巡回符号と対照される種々の符号や復号方法などが研究されている[5][7][11][18][43]．

非２進算術ＡＮ符号への拡張は，上のNeumannらの研究以外は，(3)の理由からなされたものである[10][12][37]．

本研究の目的は，対称３進表現に基づく算術演算装置．ディジタルデータ伝送路や記憶装置，さらに，これらを含む３値ディジタルシステムの高信頼化に寄与する３進算術ＡＮ符号を提案することである．それゆえ，本研究の課題は，

(1) リー距離の考えに基づく距離測度を導入し，

(2) ３進算術ＡＮ符号の誤り訂正能力を求め，

(3) その有効な復号方法を開発する．

ことにある．

１．２　概　要

本論文は，３進算術ＡＮ符号を提案し，その基礎的な理論，符号の構成と誤り検出訂正能力，さらに，復号方法について述べるものである．

符号の提案に先立って，第２章では，この符号に導入される３進の算術的な距離測度（算術重みと算術距離）を定義し，基本的な性質を示す．また，従来の算術ＡＮ符号に導入されている距離測度との概念的な相違について考察する．

第３章では，３進算術ＡＮ符号（ＳＴ－ＡＮ符号）を一般的に定義し，その基礎理論を述べる．つづいて，この符号の構成方法を示す．この方法は，生成数Aと必要とする最小距離dから符号化すべき情報整数の範囲（符号語数）を与えるものである．これにより，誤り訂正能力の小さい符号($d \leq 4$)が容易に構成できる．このような符号の情報整数の範囲は広い．誤り訂正能力が大きい符号($d>4$)の構成には電子計算機を用いて調査した．

第４章では，３進巡回算術ＡＮ符号（巡回ＳＴ－ＡＮ符号）の定義と基礎理論を述べる．まず，この符号の整数論的構造とその性質を示す．この符号は，$3^n-1=AB$の関係を満たしており，必要とする符号語数Bを与えて，符号長n，生成数Aを規定することは容易である．これにより構成された符号の最小距離を求めることは重要な問題であり，この一般的な算定方法を示し，符号語数Bが特定の条件を満たす符号の算定公式を導出する．これについては章を改め，第５章に，一連の定

理群として示すことにする．最後に，このような符号の特徴を示す．これらの定理のいくつかにより，巡回ＳＴ－ＡＮ符号がもつ誤り訂正能力の事実上の限界値が与えられる．

第６章では，３章で得られた符号のうち，巡回ＳＴ－ＡＮ符号に類似の構造をもつ負巡回ＳＴ－ＡＮ符号について述べる．これは$3^n+1=AB$を満たす符号であり，その構造や誤り訂正能力の議論に関して，巡回ＳＴ－ＡＮ符号で得られた結果の多くを利用できる．また，このような符号は，負数の表現や減算に伴う補数処理を必要とする２進表現や通常の３進表現を用いる演算においては実際的でないが，対称３進表現に基づく演算においては応用の可能性が高いと考えられる．

第７章では，これまでに提案された符号の誤り訂正の原理とそれに基づくいくつかの復号方法を提案する．巡回ＳＴ－ＡＮ符号についてはエラー・トラッピング復号の手順を示す．さらに，巡回ＳＴ－ＡＮ符号のあるものについては，代数的巡回符号の窓付きエラー・トラッピング復号[21]の考えを応用したものが有効である．この考え方に基づく誤り訂正の手順を提案する．また，この手順が有用な巡回ＳＴ－ＡＮ符号の例を求める．負巡回ＳＴ－ＡＮ符号の復号手順はこのエラー・トラッピングを応用できる．また，多数決論理復号についても，この復号方法が適用可能な巡回ＳＴ－ＡＮ符号のクラスとその復号手順を示す．

第８章では，本研究で得られた結果の総括と今後の研究方針を示す．

本論文の各章は，それぞれ，以下の文献に基づいて構成されている．

[31] Ohkura, Y., Shimada, R. and Hasegawa, T. ; "Symmetric ternary arithmetic weight and symmetric ternary arithmetic AN codes", Proc. of The 11th Int. Symp. on Multiple-Valued Logic, pp.163-167,(May. 1981)

・・・・ 第２，３，６章

[32] 大倉,島田,長谷川 ; "対称三進算術ＡＮ符号", 信学論(D), J64-D, 6, pp.

66-73,(1981)
・・・・ 第２，３，６章

[33] 大倉,島田,長谷川 ； "巡回ＳＴ－ＡＮ符号について", 信学論(D), J65-D, 11, pp.1358-1365,(1982)
・・・・ 第４，５章前半

[34] Ohkura, Y., Shimada, R. and Hasegawa, T. ; "Cyclic ST-AN codes and modular ST distance", Proc. of The 13th Int. Symp. on Multiple-Valued Logic, pp.294-299,(May. 1983)
・・・・ 第４，５章後半

[35] 大倉,島田,長谷川 ； "巡回ＳＴ－ＡＮ符号のエラー・トラッピング復号", 第６回情報理論とその応用研究会, pp.298-303,(1983)
・・・・ 第７章前半

[40] 島田,山本,青江,大倉,堀江 ； "ＨＨ型巡回ＳＴ－ＡＮ符号", 信学論(D), J66-D, 12, pp.1339-1346,(1983)
・・・・ 第７章後半

[41] 島田, 大倉, 村上 ； "多数決論理復号可能な巡回ＳＴ－ＡＮ符号", 信学論(D), J68-D, 6, pp.1218-1225,(1985)
・・・・ 第７章後半

第２章　　対称３進算術重みと対称３進算術距離

２．１　緒　言

前章でも述べたように，算術ＡＮ符号は算術演算における誤りの検出訂正を目的として開発されたものである．この符号に導入される距離測度は整数間の算術的な差に対して定義されるもので，算術距離とよばれる．とくに原点０から任意の整数Ｎまでの算術距離はＮの算術重みとよばれる．整数の２進表現に関する算術重みや算術距離は，D.T.Brown[3]により提案され，２進算術ＡＮ符号に導入された．この距離測度は，さらに，整数の非２進へ拡張され[36]，非２進算術ＡＮ符号[10][12][37]に採用されてきた．本章では，３進独特の対称３進表現に基づく３進算術重みと３進算術距離を定義する．

２．２　整数の対称３進表現と誤りの値

任意の整数Ｎの３進表現$(a_{n-1}\ \cdots\ a_1 a_0)_3$は

$$N = \sum_{i=0}^{n-1} a_i 3^i,\ (i=0,1,\cdots,n-1) \qquad (2.1)$$

を意味する．各係数a_iとして数字 $\bar{1}$,0,1を用いるものを対称３進表現あるいは簡単にST表現といい，

$$N = (a_{n-1}\ \cdots\ a_1 a_0)_{ST} \qquad (2.2)$$

で表す．ここに，$\bar{1}$ は -1 を意味する．

整数の３進表現としてST表現を用いることにより，正負の整数を対称的に表すことができる．すなわち，任意の整数Ｎが式(2.2)で表されるなら，-Ｎは，

$$-N = (\bar{a}_{n-1}\ \cdots\ \bar{a}_1 \bar{a}_0)_{ST}$$

である．ｎけたのST表現で表すことができる整数の範囲は，

$(\bar{1}\ \cdots\ \bar{1}\bar{1})_{ST} = -(3^n-1)/2$

から

$(1\ \cdots\ 11)_{ST} = (3^n-1)/2$

であり，3^n個の整数が表される．ST表現は任意の整数に対して一意に定まることは明らかである．

整数のST表現の一部を表２．１に例示する．同時に，式(2.1)の係数a_iとして，数字0,1,2を用いるよく知られた３進表現（以下，簡単にM3表現という）も示す．

３進算術ＡＮ符号において用いられてきた算術重みは，式(2.1)の係数に数字$\bar{2},\bar{1},0,1,2$を用いる一般化された３進表現（以下，簡単にGT表現という）を介して定義されるもので，これをMT算術重み[15]ということにする．すなわち，整数ＮのMT算術重み$W_{MT}(N)$は，ＮのGT表現のうち非零けたの個数が最小となるいわゆる最小重み表現(非隣接表現あるいはNAF)[36]における非零けたの個数で与えられるものである．

整数ＮのST表現の3^iのけたに誤りが生じて別の整数Ｍに変化したとする．このとき，その差Ｍ－Ｎは，

$M-N = b_i 3^i,\ b_i \in \{\bar{2},\bar{1},0,1,2\}$

で表すことができる．MT算術重みの定義によれば，１けたで生じた誤りの値$b_i = \pm 1, \pm 2$は すべて重み1の誤りとして取り扱う（図２．１(a)参照）．これは代数的符号で用いられるハミング重み[17]の概念に基づくものであり，誤りの値±1と±2の発生確率が相等しいような回路方式が採られている算術演算装置や通信路に適している．しかし，整数のST表現で使用される数字 $\bar{1},0,1$を電圧や電流の３レベルで表すような多レベル信号方式の場合，誤りの値±2の発生確率は誤りの値±1のそれよりも著しく小さいと考えられる．このため，誤りの値±2は±1より大きい重みを持たせるほうがより合理的である．以上のことから，図２．１(b)に示すように誤りの値±2をそのST表現$1\bar{1}/\bar{1}1$なる２けたに及ぶ誤りとして取り扱うことにする．これは，非２値の代数的符号で導入されているリー重み[22]が１けたにおける誤りの大きさまで考慮するという点で，このリー重みの概念を算術重みへ拡張したものと考えられる．

２．３　算術重みと算術距離

［定義２．１］　任意の整数$N=(a_{n-1}\ \cdots\ a_1a_0)_{ST}$のST算術重み$W_{ST}(N)$を

$$W_{ST}(N)=\sum_{i=0}^{n-1}|a_i|,\ (i=0,1,\cdots,n-1) \tag{2.3}$$

とする．

整数NのST表現において，各けたa_iの絶対値$|a_i|$は 0 または 1 であるから$W_{ST}(N)$はNのST表現の非零けたの個数に等しい．

ST算術重み$W_{ST}(N)$はつぎの性質をもつ．

［性質２．１］　$W_{ST}(N)\geqq 0$ (2.4)

［性質２．２］　$W_{ST}(-N)=W_{ST}(N)$ (2.5)

［性質２．３］　$W_{ST}(N+M)\leqq W_{ST}(N)+W_{ST}(M)$ (2.6)

（証明）　不等式(2.4)はST算術重みの定義により明らかである．　ただし．$W_{ST}(N)=0$となるのは，$N=0$のときに限る．式(2.5)はST表現の対称性とST算術重みの定義により，$N=(a_{n-1}\ \cdots\ a_1a_0)_{ST}$のとき，

$$W_{ST}(N)=\sum_{i=0}^{n-1}|a_i|=\sum_{i=0}^{n-1}|\bar{a}_i|=W_{ST}(-N).$$

性質２．３を証明するために，N,MおよびN＋Mをそれぞれ，$N=(a_{n-1}\ \cdots\ a_1a_0)_{ST}$，$N=(b_{n-1}\ \cdots\ b_1b_0)_{ST}$，$N+M=(c_ns_{n-1}\ \cdots\ s_1s_0)_{ST}$とする．第iけたにおける加算$a_i+b_i+c_i=c_{i+1}s_i$を考える．ここに，$c_i$,$c_{i+1}$はそれぞれ第i-1けたから第iけた，第iけたから第i+1けたへのけた上げであり，c_i,c_{i+1} は0または±1である．$-1\leqq a_i+b_i+c_i\leqq 1$のとき，$c_{i+1}=0$，$s_i=a_i+b_i+c_i$であり，

$$|c_{i+1}|+|s_i|=|a_i+b_i+c_i|\leqq|a_i|+|b_i|+|c_i|,$$

$-3\leqq a_i+b_i+c_i\leqq -2$のとき，$c_{i+1}=-1$，$s_i=a_i+b_i+c_i+3$であり，

$$|c_{i+1}|+|s_i|=1+|a_i+b_i+c_i+3|$$

$$\leqq 2 \leqq |a_i+b_i+c_i| \leqq |a_i| + |b_i| + |c_i| .$$

$2 \leqq a_i+b_i+c_i \leqq 3$のとき，$c_{i+1}=1, s_i=a_i+b_i+c_i-3$であり，

$$|c_{i+1}| + |s_i| = 1 + |a_i+b_i+c_i-3|$$
$$\leqq 2 \leqq |a_i+b_i+c_i| \leqq |a_i| + |b_i| + |c_i| .$$

いずれにしても，不等式

$$|c_{i+1}| + |s_i| \leqq |a_i| + |b_i| + |c_i|$$

が成立する．すべての$i(=0,1,\cdots,n-1)$についてこれらの不等式を加え合わせることにより，

$$W_{ST}(N+M) = |c_n| + \sum_{i=0}^{n-1} |s_i|$$

$$\leqq \sum_{i=0}^{n-1} (|a_i| + |b_i|) = W_{ST}(N)+W_{ST}(M)$$

を得る．　（証明終）

ST表現の基数（Radix）は3で奇数であることから，整数NのST算術重みとN自身の間に次の関係が成立する．

[性質２．４]　$W_{ST}(N) \equiv N \pmod 2$　　(2.7)

（証明）　NのST表現$(a_{n-1}\cdots a_1 a_0)_{ST}$の非零けた$a_i$に着目する．$|a_i|=1$であるから，ST算術重みの定義により，非零けたが奇数個あれば，$N, W_{ST}(N)$ともに奇数であり，偶数個あれば，$N, W_{ST}(N)$ともに偶数である．　（証明終）

[性質２．５]　$W_{ST}(3^{n+1}-K) = W_{ST}(3^n+K) = W_{ST}(K)+1,$
$(K=0,1,\cdots,3^n,\ n=1,2,3,\cdots).$　　(2.8)

（証明）　K は n+1けた以下のST表現で表され，$K=(a_n a_{n-1} \cdots a_0)_{ST}$とすると，$a_n$は 0 または 1 である．いずれの場合も，$W_{ST}(3^{n+1}-K)=W_{ST}(K)+1$である．$3^n+K$のST表現を$(b_{n+1} b_n \cdots b_0)_{ST}$とすると，$b_0=a_0, b_1=a_1, \cdots, b_{n-1}=a_{n-1}$で

ある．$a_n=0$のとき，$b_n=1, b_{n+1}=0$．$a_n=1$のとき，$b_n=\bar{1}, b_{n+1}=1$．それゆえ，$W_{ST}(3^n+K)=W_{ST}(K)+1$である．　　（証明終）

この性質２．５を用いて連続する整数のST算術重みを漸化的に求めることができる．すなわち，$W_{ST}(0)$～$W_{ST}(3^n)$が与えられているとき，式(2.8)により，$W_{ST}(3^n+1)$～$W_{ST}(2x3^n)$が得られ，さらに$W_{ST}(2x3^n+1)$～$W_{ST}(3^{n+1})$が整数の大きいほうから順次得られる．したがって，初期値として$W_{ST}(0)=0, W_{ST}(1)=1, W_{ST}(2)=2, W_{ST}(3)=1$を与えれば，連続する整数のST算術重みを図２．２のように求めることができる．

［定義２．２］　整数MからNまでのST算術距離$D_{ST}(M,N)$を

$$D_{ST}(M,N) = W_{ST}(N-M) \qquad (2.9)$$

とする．

このとき，$D_{ST}(M,N)$は次の基本的な性質をもつメトリック関数である．

［性質２．６］　$D_{ST}(M,N) \geqq 0$　　(2.10)

［性質２．７］　$D_{ST}(M,N) = D_{ST}(N,M)$　　(2.11)

［性質２．８］　$D_{ST}(M,N) \leqq D_{ST}(M,L) + D_{ST}(L,N)$　　(2.12)

（証明）　性質２．６，２．７については，$D_{ST}(M,N)$の定義と$W_{ST}(N)$の性質２．１～２により，容易に証明することができる．性質２．８は，$W_{ST}(N)$に関する三角不等式（性質２．３）を用いて，

$$\begin{aligned} D_{ST}(M,N) &= W_{ST}(N-M) \\ &= W_{ST}(L-M+N-L) \\ &\leqq W_{ST}(L-M) + W_{ST}(N-L) \\ &= D_{ST}(M,L) + D_{ST}(L,N) \end{aligned}$$

を得る．　　（証明終）

２．４　整数の３進表現と算術重み

任意の整数ＮのST算術重み$W_{ST}(N)$は，定義２．１により，ＮのST表現から直接得られるものである．本節では，ST算術重みとMT算術重みとの違いをより明確にするために，算術重みの概念（図２．１(b)）に基づくST算術重みをMT算術重みと同様の手順によりGT表現から導く．

整数ＮのGT表現を

$$N=(b_{m-1}\ \cdots\ b_1 b_0)_{GT},\quad (b_i\in\{\bar{2},\bar{1},0,1,2\}\ ,i=0,1,\cdots,m-1) \tag{2.13}$$

で表す．ＮのGT表現は一意ではないが，各けたの絶対値 $|b_i|$ のすべての和が最小となるような表現が存在する．これをST最小重み表現ということにする．これはMT算術重みを求める際に導入される最小重み表現に対応するものである．

［定理２．１］　任意の整数ＮのST算術重みはＮのST最小重み表現における各けたの絶対値の和に等しい．

（証明）　整数ＮのST最小重み表現のひとつを$N=(b_{m-1}\ \cdots\ b_1 b_0)_{GT}$で表す．このとき，各けた$b_i$の絶対値の和Ｓ(Ｎ)は，

$$S(N)=\sum_{i=0}^{m-1}|b_i| \tag{2.14}$$

であり，GT表現における各けた絶対値の和の最小値である．ＮのST最小重み表現のすべてのけた$b_i(i=0,1,\cdots,m-1)$に対して，

$b_i=0,1,\bar{1}$のとき，　$x_i=b_i$，　$y_{i+1}=0$

$b_i=2,\bar{2}$ のとき，　$x_i=\bar{b}_i/2$，　$y_{i+1}=b_i/2$

とする．これらのx_i,y_{i+1}を用いてふたつの整数

$N_x=(x_{m-1}\ \cdots\ x_1 x_0)_{ST}$，

$N_y=(y_m y_{m-1}\ \cdots\ y_1 y_0)_{ST},(y_0=0)$

を得る．このとき，

$$N = N_x + N_y \qquad (2.15)$$

である．　NのST最小重み表現において，$b_i = \pm 2$であるけたの個数をjとすれば，N_x，N_yのST算術重みはそれぞれ，

$$W_{ST}(N_x) = S(N) - j,\ W_{ST}(N_y) = j \qquad (2.16)$$

である．式(2.15)，(2.16)およびST算術重みの性質２．３により，

$$S(N) = W_{ST}(N_x) + W_{ST}(N_y) \geqq W_{ST}(N)$$

が成立する．S(N)の定義により，$S(N) = W_{ST}(N)$である．　（証明終）

上の定理は，NのST表現がNのST最小重み表現のひとつであり，ST表現それ自身がMT算術重みで用いられる最小重み表現に対応していることを示している．すなわち，整数NのMT算術重みが非零けたの個数最小となるGT表現に基づくものであるのに対して，ST算術重みは各けたの絶対値の和が最小となるようなGT表現に基づいていると考えることができる．

２．５　モジュラ重みとモジュラ距離

任意の整数Nの法mに関する絶対最小剰余を $N \bmod m$ で表す．また，法mに関する絶対最小完全剰余系をZ_mで表す．ここに，mが奇数なら，

$$Z_m = \{0, \pm 1, \pm 2, \cdots, \pm (m-1)/2\}$$

であり，mが偶数なら，

$$Z_m = \{0, \pm 1, \pm 2, \cdots, \pm (m-2)/2, m/2\}$$

である．このZ_mは法mに関して加算と乗算のもとに環をなす．

［定義２．３］　整数NのモジュラST重みを

$$W_{mST}(N) = W_{ST}(N \bmod m) \qquad (2.17)$$

とする．

整数NがZ_mに属するなら，Nのモジュラ重みは NのST算術重みに一致する．すなわち，$W_{mST}(N) = W_{ST}(N)$である．

［定義２．４］　Z_mに属する整数M,Nに対して，MからNまでのモジュラST距離を

$$D_{MST}(M,N) = W_{MST}(N-M) \qquad (2.18)$$

とする．

モジュラ距離の概念はT.R.N.Rao[38]により提案されたものであるが，これは法mに関する負でない最小完全剰余系である整数の有限環上での算術距離を定義したものである．ここに定義したモジュラST距離は法mに関する絶対最小完全剰余系（整数の有限環）の上でのものである．

以下では，m が 3^n-1 と 3^n+1 の形で表されるとき，この２種類のモジュラST距離について考える．これら２種類のモジュラST距離は，ST算術距離の基本的な性質２．６～２．８と同様な性質をもつメトリック関数である．すなわち，法$m=3^n\pm1$に関する絶対最小完全剰余系Z_m上で定義されるモジュラST距離について次の性質が成り立つ．

［性質２．９］　$D_{MST}(M,N) \geqq 0$ (2.19)

［性質２．10］　$D_{MST}(M,N) = D_{MST}(N,M)$ (2.20)

［性質２．11］　$D_{MST}(M,N) \leqq D_{MST}(M,L)+D_{MST}(L,N)$ (2.21)

（証明）　不等式(2.19)および式(2.20)はST重みの性質２．１，２．２およびモジュラST重み，モジュラST距離の定義により容易に証明される．性質２．11を証明するために，Z_mに属する任意の整数M,Nに対して，

$$W_{MST}(M+N) \leqq W_{MST}(M)+W_{MST}(N) \qquad (2.22)$$

が成立することを示す．$m=3^n-1$の場合，整数M,Nは，Z_mの元であるから，これらの整数のST表現はnけたで表される．$m=3^n+1$の場合，nけたで表現できないZ_mの元がただ一個存在するが，それは$(3^n+1)/2=(1\bar{1}\bar{1}\cdots\bar{1})_{ST}$である．したがって，いずれの場合も，算術和M+NのST表現は，(n+1)けたを越えることはなく，

$$M+N=(c_n s_{n-1}\cdots s_1 s_0)_{ST}$$

のように表せる．算術和M+NがZ$_m$に属するなら，ST算術重みの性質２．３により，

$$W_{MST}(M+N) = W_{ST}(M+N)$$
$$\leqq W_{ST}(M)+W_{ST}(N) = W_{MST}(M)+W_{MST}(N)$$

である．算術和M+NがZ$_m$に属さないなら，$c_n = \pm 1$である．

$$(M+N) \bmod (3^n \pm 1) = M+N-c_n(3^n \pm 1)$$
$$= (s_{n-1} \cdots s_1 s_0)_{ST} \mp c_n$$

である．したがって，ST算術重みの性質により，

$$W_{MST}(M+N) = W_{ST}((M+N) \bmod (3^n \pm 1))$$
$$\leqq W_{ST}(M+N-c_n 3^n)+W_{ST}(\mp c_n)$$
$$\leqq W_{ST}(M+N)-1+1$$
$$\leqq W_{ST}(M)+W_{ST}(N) = W_{MST}(M)+W_{MST}(N)$$

である．このため，性質２.11はこのモジュラST重みに関する不等式を用いて，性質２．８の場合と同様にして証明できる．　（証明終）

２．６　結　言

本章では，整数の対称３進表現に基づく算術重み（ST算術重み）と算術距離（ST算術距離）を定義し，それらの基本的な性質を示した．さらに，この距離測度の概念に基づき，正整数mを法とする絶対最小完全剰余系の有限な環上でモジュラST重みとモジュラST距離を定義し，とくに，m が $3^n \pm 1$ の場合について，モジュラST距離がメトリック関数であることを示した．

表２．１　整数ＮのST表現

N	M3 表現	ST 表現
0	0 0 0 0	0 0 0 0
1	0 0 0 1	0 0 0 1
2	0 0 0 2	0 0 1 $\bar{1}$
3	0 0 1 0	0 0 1 0
4	0 0 1 1	0 0 1 1
5	0 0 1 2	0 1 $\bar{1}$ $\bar{1}$
6	0 0 2 0	0 1 $\bar{1}$ 0
7	0 0 2 1	0 1 $\bar{1}$ 1
8	0 0 2 2	0 1 0 $\bar{1}$
9	0 1 0 0	0 1 0 0
10	0 1 0 1	0 1 0 1
11	0 1 0 2	0 1 1 $\bar{1}$
12	0 1 1 0	0 1 1 0
13	0 1 1 1	0 1 1 1
14	0 1 1 2	1 $\bar{1}$ $\bar{1}$ $\bar{1}$
15	0 1 2 0	1 $\bar{1}$ $\bar{1}$ 0
16	0 1 2 1	1 $\bar{1}$ $\bar{1}$ 1
17	0 1 2 2	1 $\bar{1}$ 0 $\bar{1}$
18	0 2 0 0	1 $\bar{1}$ 0 0
19	0 2 0 1	1 $\bar{1}$ 0 1
20	0 2 0 2	1 $\bar{1}$ 1 $\bar{1}$
21	0 2 1 0	1 $\bar{1}$ 1 0
22	0 2 1 1	1 $\bar{1}$ 1 1
23	0 2 1 2	1 0 $\bar{1}$ $\bar{1}$
24	0 2 2 0	1 0 $\bar{1}$ 0
25	0 2 2 1	1 0 $\bar{1}$ 1
26	0 2 2 2	1 0 0 $\bar{1}$
27	1 0 0 0	1 0 0 0
⋮	⋮	⋮
⋮	⋮	⋮

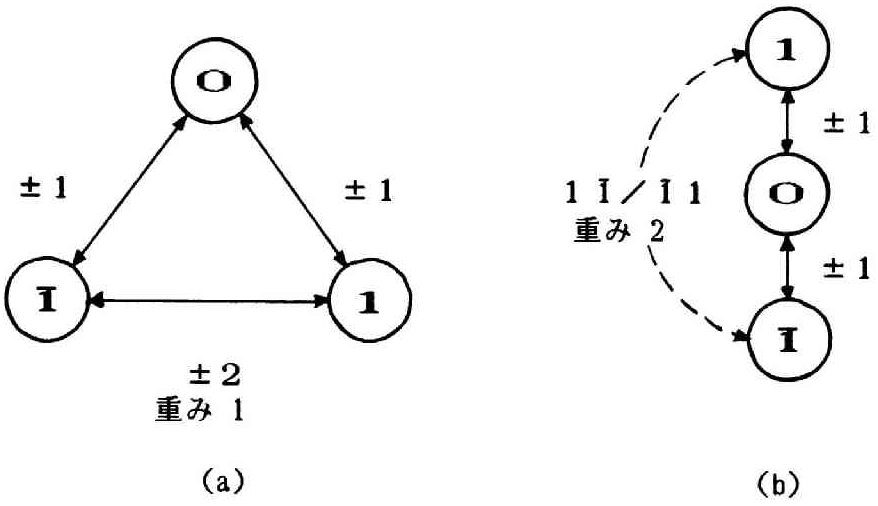

図２．１　整数のST表現の１けたにおける誤りの値と重み
（a）　MT算術重み　　（b）　ST算術重み

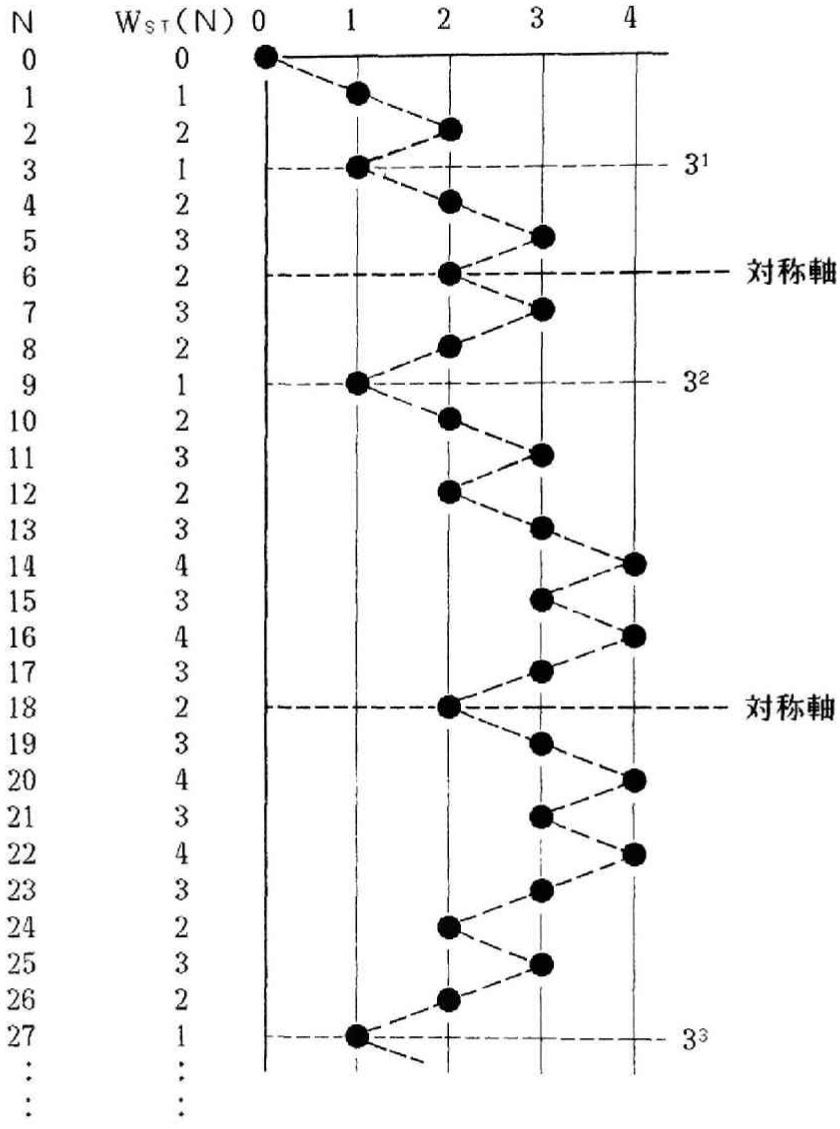

図２．２　連続する整数のST算術重みの変化

第３章　　ＳＴ－ＡＮ符号

３．１　緒　言

本章では，対称３進表現に基づく算術ＡＮ符号（ＳＴ－ＡＮ符号）の基礎理論について述べる．この符号に対して，前章で定義したST算術重みやST算術距離が導入される．符号の構成において，重要なパラメータが定義される．これは，最小距離と生成数から情報整数の範囲を与えるものである．このパラメータを用いて，情報整数の範囲を求める方法を検討する．

３．２　ＳＴ－ＡＮ符号

算術ＡＮ符号は特定の正整数Aの整数倍ANからなる集合であり，Nは符号語ANに符号化すべき情報整数である．このとき，この符号はAによって生成されるといい，Aを生成数という．すべての符号語ANがST表現されているとき，この符号をＳＴ－ＡＮ符号という．生成数Aが基数3の倍数であれば，すべての符号語ANの少なくとも最下位のけたが0となり，無意味な冗長けたを生じる．これは不都合であるから，以下では，Aは3と互いに素，すなわち，(A,3)=1となるように選ぶものとする．

Aで生成されるＳＴ－ＡＮ符号のすべての相異なる符号語間のST算術距離の最小値d_mをこの符号の最小距離という．生成数Aとの積のST算術重みがd未満となる最小の正整数を$M_{ST}(A,d)$で表す．言い換えれば，$|M| < M_{ST}(A,d)$を満たすどのような非零整数Mも，Aとの積のST算術重み$W_{ST}(AM)$がd以上となる．

［定理３．１］　情報整数Nの範囲を

$$-\frac{M_{ST}(A,d)}{2} < N < \frac{M_{ST}(A,d)}{2} \qquad (3.1)$$

に限れば，Aで生成されるＳＴ－ＡＮ符号の最小距離d_mはd以上である．

（証明）式(3.1)を満たす任意の相異なる整数N_1,N_2に対して，不等式 $|N_1-N_2|<M_{ST}(A,d)$が成立する．したがって，$M_{ST}(A,d)$の定義により，

$$D_{ST}(AN_1,AN_2) = W_{ST}(AN_2-AN_1)$$
$$= W_{ST}(A(N_2-N_1)) \geqq d$$

である． （証明終）

[定理３．２] 生成数Aが偶数であって，最小重みdが奇数なら，

$$M_{ST}(A,d) = M_{ST}(A,d+1) \qquad (3.2)$$

（証明） Aが偶数なら，ST算術重みの性質２．４により，ANおよび$W_{ST}(AN)$は共に偶数である．$0 < |N| < M_{ST}(A,d)$なる範囲の整数Nに対して，$W_{ST}(AN)$の値はd未満ではなく，さらにdでもない． （証明終）

３．３ 最小距離と誤り訂正能力

算術ＡＮ符号において取り扱う誤りは，符号語に算術的に加えられる正または負の整数である．その結果としてけた上げを生じることがあるが，このような誤りを算術誤りという．本章では，取り扱う算術誤りEの範囲を

$$-\frac{AM_{ST}(A,d)}{2} < E < \frac{AM_{ST}(A,d)}{2} \qquad (3.3)$$

とする．符号語ANに算術誤りEが生じて受信語V=AN+Eを得たとする．このとき，ANからVまでのST算術距離は

$$D_{ST}(AN,V) = W_{ST}(V-AN) = W_{ST}(E) \qquad (3.4)$$

で与えられる．$W_{ST}(E)=t$のとき，Eをt重の算術誤りあるいは簡単にt重誤りという．

[定理３．３] ＳＴ－ＡＮ符号の最小距離が d+1 以上であれば，式(3.3)の範囲のd重以下のすべての算術誤りを検出することができる．

（証明） AN_1を任意の符号語とし，Eを式(3.3)の範囲のd重以下の任意の算術誤りとする．受信語$V=AN_1+E$がある符号語AN_2に一致したと仮定すると，

$$D_{ST}(AN_1, AN_2) = W_{ST}(AN_2 - AN_1) = W_{ST}(E) \leqq d$$

である．これは，この符号の最小距離がd+1以上という仮定に反する．それゆえ，Vは符号語に一致することはなく，Eは検出可能である．　　（証明終）

［定理３．４］　ＳＴ－ＡＮ符号の最小距離が 2t+1 以上であれば，式(3.3)の範囲のt重以下のすべての算術誤りを訂正することができる．

（証明）　相異なる任意の符号語AN_1, AN_2に対して，$AN_1+E_1=AN_2+E_2$を満たすt重以下の算術誤りE_1, E_2が存在しなければ，受信語$V_1=AN_1+E_1$に符号語AN_1を一意に対応させることができる．E_1, E_2が存在すると仮定すると，性質２．３により，

$$\begin{aligned} D_{ST}(AN_1, AN_2) &= W_{ST}(AN_2 - AN_1) \\ &= W_{ST}(E_1 - E_2) \\ &\leqq W_{ST}(E_1) + W_{ST}(E_2) \\ &\leqq 2t \end{aligned}$$

である．これは，この符号の最小距離が2t+1以上であるという仮定に反する．

（証明終）

［系３．１］　ＳＴ－ＡＮ符号の最小距離が d+t+1(>2t+1) 以上であれば，式(3.3)の範囲のすべてのt重以下の算術誤りを訂正し，同じ範囲のすべてのd重以下の算術誤りを検出することができる．　　（証明略）

３．４　最小距離と情報整数の範囲

必要とする誤り検出訂正能力が与えられるとき，ある整数Aで生成されるＳＴ－ＡＮ符号の情報整数の範囲は，パラメータ$M_{ST}(A,d)$を求めることにより，定理３．１から与えられる．ＳＴ－ＡＮ符号を構成する際，このパラメータを求めること

は重要な問題である．

３．４．１　最小距離2の符号（$M_{ST}(A,2)$）

［定理３．５］　生成数Aが3と互いに素ならば，

$$M_{ST}(A,2) = \infty \qquad (3.5)$$

である．

（証明）　ST算術重みが1である整数はすべて$\pm 3^i$と表すことができる．Aは3と互いに素であるから，Aは$\pm 3^i$を整除することはあり得ない．さらに，どのような整数Nもこのようなとの積ANが$\pm 3^i$に等しくなることはない．すなわち，任意の非零整数Nに対してANのST重みは2以上である．　（証明終）

上の定理の条件を満たす最小の正整数Aは2である．A=2で生成されるＳＴ－ＡＮ符号はすべての情報整数Nに対して最小距離2をもつ．このことはST算術重みの性質２．４からも容易に知ることができる．すなわち，0以外の任意の符号語2NのST算術重みは2以上の偶数である．

３．４．２　最小距離3の符号（$M_{ST}(A,3)$）

法Aに関して3が属するべき数をE(3,A)で表す．Aが3と互いに素ならば，$3^e-1\equiv 0(\mathrm{mod}\ A)$を満たす最小の正整数eが存在する．　このとき，e=E(3,A)である．また，$3^g+1\equiv 0(\mathrm{mod}\ A)$を満たす最小の正整数g が存在するなら，このようなgをG(3,A)で表す．

［補題３．１］　G(3,A)が存在するなら，

$$G(3,A) = E(3,A)/2 \qquad (3.6)$$

である．

（証明）　G(3,A)が存在するなら，$3^{2G(3,A)}-1\equiv 0\ (\mathrm{mod}A)$である．それゆえ，

E(3,A)は2G(3,A)を整除しなければならないから，2G(3,A)=kE(3,A)なる整数kが存在する．明らかに，G(3,A)＜E(3,A)であるから，kは1でなくてはならない．

（証明終）

G(3,A)が存在するのはE(3,A)が偶数でなければならないが，E(3,A)が偶数であってもG(3,A)が存在するとは限らない．もちろん,E(3,A)が奇数なら，G(3,A)は存在しない．3と互いに素な正整数A(2≦A≦121)のE(3,A)およびG(3,A)を表３．１に示す．

［定理３．６］　生成数Aは3と互いに素とする．G(3,A)が存在するなら，

$$M_{ST}(A,3) = (3^{G(3,A)}+1)/A \qquad (3.7)$$

G(3,A)が存在しないなら，

$$M_{ST}(A,3) = (3^{E(3,A)}-1)/A \qquad (3.8)$$

である．

（証明）　Aが3と互いに素であるから，定理３．５により，$M_{ST}(A,3)$が存在するなら．$AM_{ST}(A,3)$のST算術重みは1でなく2に限られる．ST算術重みが2である整数はすべて$\pm 3^j(3^i \pm 1)$と表すことができる．(A,3)=1 であるから，ANが $\pm 3^j(3^i \pm 1)$で表すことができる最小の正整数は $3^i \pm 1$ である．Aが整除する $3^i \pm 1$ なる形の最小の正整数は，補題３．１により，G(3,A)が存在するとき，$3^{G(3,A)}+1$ であり，G(3,A)が存在しないとき，$3^{E(3,A)}-1$ である．　（証明終）

例３．１　A=91のとき，法91に関して，

$3^1 \equiv 3,\ 3^2 \equiv 9,\ 3^3 \equiv 27,\ 3^4 \equiv -10,\ 3^5 \equiv -30,\ 3^6 \equiv 1$

であるから，E(3,91)=6であり，G(3,91)は存在しない．式(3.8)により，

$$M_{ST}(91,3) = (3^6-1)/91 = 8$$

を得る．このため，情報整数Nを$-3 \leqq N \leqq 3$に限れば，A=91で生成されるＳＴ－ＡＮ符号の最小距離d_mは3以上である．実際，

$91\times1 = (010101)_{ST}$　　$91\times5 = (1\bar{1}0\bar{1}0\bar{1}\bar{1})_{ST}$

$91\times2 = (1\bar{1}1\bar{1}1\bar{1})_{ST}$　　$91\times6 = (1\bar{1}1\bar{1}1\bar{1}0)_{ST}$

$91\times3 = (101010)_{ST}$　　$91\times7 = (10\bar{1}0\bar{1}\bar{1}1)_{ST}$

$91\times4 = (111111)_{ST}$　　$91\times8 = (100000\bar{1})_{ST}$

であり，d_m=3である．

表３．１に示したようなE(3,A)およびG(3,A)の一覧表と定理３．６を用いて，与えられた要件を満たす最小距離3のＳＴ－ＡＮ符号を探すことができる．

以下では，生成数Aが5以上の素数の場合を考える．

［補題３．２］　pは5以上の素数とする．法pに関して3が原始根なら，

$$G(3,p) = E(3,p)/2 = (p-1)/2 \qquad (3.9)$$

である．

（証明）　pが5以上の素数であって，法pに関して3が原始根であるから，法pに関して3が属するべき数E(3,p)とpのオイラー関数$\varphi(p)$=p-1が等しい．また，p-1は偶数であるから，

$$\begin{aligned} 3^{E(3,p)}-1 &= 3^{p-1}-1 \\ &= (3^{(p-1)/2}+1)(3^{(p-1)/2}-1) \\ &\equiv 0 \pmod p \end{aligned}$$

である．法pに関して3が原始根であるから，$3^{(p-1)/2}$は法pに関して1に合同ではあり得ない．このため，$3^{(p-1)/2}\equiv -1 \pmod p$でなくてはならない．それゆえ，G(3,p)が存在して，G(3,p)=E(3,p)/2=(p-1)/2である．　（証明終）

［補題３．３］　mは3と互いに素な正整数とする．法mに関して3でなく-3が原始根なら，

$$E(3,m) = \varphi(m)/2 \qquad (3.10)$$

であり，これは奇数であって，G(3,m)は存在しない．

（証明）　法mに関して3が原始根でないから，E(3,m)≦φ(m)/2である．　E(3,m)<φ(m)/2 と仮定すると，

$$(-3)^{2E(3,m)} = 3^{2E(3,m)} \equiv 1 \pmod{m}$$

となり，これは法mに関して-3が原始根であることに矛盾する．　したがって，E(3,m)=φ(m)/2である．これが偶数なら，

$$(-3)^{\varphi(m)/2} = 3^{\varphi(m)/2} \equiv 1 \pmod{m}$$

となり，-3が原始根であることに矛盾する．したがって，E(3,m)は奇数である．

（証明終）

上の補題においてmが5以上の素数pの場合，オイラー関数φ(p)=p-1であるから，E(3,p)＝(p-1)/2である．

［定理３．７］　生成数A=pは5以上の素数とする．法pに関して3が原始根なら，

$$M_{ST}(p,3) = (3^{(p-1)/2}+1)/p \qquad (3.11)$$

である．また，法pに関して3でなく-3が原始根なら，

$$M_{ST}(p,3) = (3^{(p-1)/2}-1)/p \qquad (3.12)$$

であり，これらは共に偶数である．　（証明略）

以上の定理で与えられる$M_{ST}(A,3)$の代表的な値を表３．２に示す．

例３．２　A=p=11のとき，法11に関して3でなく-3が原始根である．実際，法11に関して，

$$3^1 \equiv 3,\ 3^2 \equiv -2,\ 3^3 \equiv 5,\ 3^4 \equiv 4,\ 3^5 \equiv 1$$

であり，E(3,11)=5，また，

$$(-3)^1 \equiv -3,\ (-3)^2 \equiv -2,\ (-3)^3 \equiv -5,\ (-3)^4 \equiv 4,\ (-3)^5 \equiv -1,$$

$$(-3)^6 \equiv 3\ ,\ (-3)^7 \equiv 2\ ,\ (-3)^8 \equiv 5\ ,\ (-3)^9 \equiv -4,(-3)^{10} \equiv 1$$

であり，E(-3,11)=10である．式(3.12)により，

$$M_{ST}(11,3) = (3^5-1)/11 = 22$$

であり，Nを-10≦N≦10に限れば，A=11で生成されるＳＴ－ＡＮ符号の最小距離d_mは3以上である．実際，

$11\times 1 = (00111\bar{1})_{ST}$　　$11\times 12 = (1\bar{1}\bar{1}0\bar{1}0)_{ST}$

$11\times 2 = (01\bar{1}11)_{ST}$　　$11\times 13 = (1\bar{1}\bar{1}10\bar{1})_{ST}$

$11\times 3 = (011\bar{1}0)_{ST}$　　$11\times 14 = (1\bar{1}0\bar{1}01)_{ST}$

$11\times 4 = (1\bar{1}\bar{1}0\bar{1})_{ST}$　　$11\times 15 = (1\bar{1}0010)_{ST}$

$11\times 5 = (1\bar{1}001)_{ST}$　　$11\times 16 = (1\bar{1}1\bar{1}\bar{1}\bar{1})_{ST}$

$11\times 6 = (1\bar{1}110)_{ST}$　　$11\times 17 = (1\bar{1}10\bar{1}1)_{ST}$

$11\times 7 = (100\bar{1}\bar{1})_{ST}$　　$11\times 18 = (1\bar{1}1100)_{ST}$

$11\times 8 = (101\bar{1}1)_{ST}$　　$11\times 19 = (10\bar{1}\bar{1}1\bar{1})_{ST}$

$11\times 9 = (11\bar{1}00)_{ST}$　　$11\times 20 = (10\bar{1}011)_{ST}$

$11\times 10 = (1101\bar{1})_{ST}$　　$11\times 21 = (100\bar{1}\bar{1}0)_{ST}$

$11\times 11 = (11111)_{ST}$　　$11\times 22 = (10000\bar{1})_{ST}$

であり，d_m=3である．

３．４．３　最小距離4の符号（$M_{ST}(A,4)$）

生成数Aが偶数の場合，定理３．２により，$M_{ST}(A,4)=M_{ST}(A,3)$である．このことを利用して，$M_{ST}(A,4)$を与える公式を導く．以下，pは5以上の素数とする．はじめに，生成数A=2pの場合を考える．

［補題３．４］　pは5以上の素数とする．法pに関して3が原始根であるとき，そのときに限って，3は法2pに関する原始根である．また，法pに関して-3が原始根であるとき．そのときに限って，-3は法2pに関する原始根である．

（証明）　法pに関して3が原始根，すなわち，$E(3,p)=\varphi(p)=p-1$とする．法2p

に関して3が属するべき数をE(3,2p)とすると，

$$3^{E(3,2p)}-1 \equiv 0 \pmod{2p}$$

であるから，上式の左辺は法pに関しても

$$3^{E(3,2p)}-1 \equiv 0 \pmod{p}$$

である．このため，E(3,p)=p-1はE(3,2p)を整除する．同時に，E(3,2p)は$\varphi(2p)$を整除するから，E(3,2p)=p-1=$\varphi(2p)$である．逆に，法2pに関して3が原始根であるとする．このとき，

$$3^{E(3,p)} = kp+1$$

なる正整数kが存在し，左辺が奇数であるから，kは偶数であり，k=2k'なる正整数k'が存在する．したがって，

$$3^{E(3,p)}-1 = k'(2p) \equiv 0 \pmod{2p}$$

であるから，E(3,2p)=p-1=$\varphi(p)$ はE(3,p)を整除する．同時に，E(3,p)は$\varphi(p)$=p-1を整除するから，E(3,p)=$\varphi(p)$である．以上で定理の前半が証明された．他方，法pに関して-3が原始根の場合についても上と同様にして証明される．

（証明終）

［補題３．５］　pは5以上の素数とする．法pに関して3が原始根なら，

$$G(3,2p) = (p-1)/2 \qquad (3.13)$$

である．

（証明）　法pに関して3が原始根であるから，補題３．４により，3は法2pに関する原始根である．それゆえ，整数kが1からp-1までを変わるとき，$3^k \bmod 2p$は法2pに関する既約剰余系の元（p-1=$\varphi(2p)$個のp以外の奇数）を丁度１通りだけ変わる．このとき，$3^g \equiv -1 \pmod{2p}$ なる正整数gが存在し，補題３．１により，g=G(3,2p)=E(3,2p)/2=(p-1)/2である．　（証明終）

［補題３．６］　pは5以上の素数とする．法pに関して3でなく-3が原始根なら，

$$E(3,2p) = (p-1)/2 \qquad (3.14)$$

であり，これは奇数であって，G(3,2p)は存在しない．

（証明）　法pに関して3でなく-3が原始根であるとする．補題３．４により，法2pに関して-3が原始根であり，3は原始根でない．したがって，補題３．３と同様にして証明される．　（証明終）

補題３．４～３．６および定理３．２．３．６により，次の定理が導かれる．

［定理３．８］　pが5以上の素数で，生成数A=2pとする．法pに関して3が原始根であるなら，

$$M_{ST}(2p,4) = (3^{(p-1)/2}+1)/(2p) \qquad (3.15)$$

また，法pに関して3でなく-3が原始根であるなら，

$$M_{ST}(2p,4) = (3^{(p-1)/2}-1)/(2p) \qquad (3.16)$$

である．　（証明略）

例３．３　A=2p=2×11のとき，法11に関して3でなく-3が原始根であるから，式(3.16)により，

$$M_{ST}(22,4)=(3^5-1)/22=11$$

である．Nを-5≦N≦5に限れば，A=22で生成されるＳＴ－ＡＮ符号の最小距離は4以上である．実際，この符号のすべての符号語は，例３．２のA=11で生成される最小距離3のＳＴ－ＡＮ符号の情報整数が偶数の場合の符号語に一致するから，その例からも明らかなように，この符号の最小距離はd_m=4である．

つぎに，生成数A=4pの場合を考える．このとき，4pの位数は

$$\varphi(4p) = 2(p-1)$$

である．法pに関して3が原始根である場合と3でなく-3が原始根である場合に分けて考えるが，いずれにしても法4pに関する原始根は存在しない．

［補題３．７］　法pに関して3が原始根であり，4がp-1を整除するなら，

$$E(3,4p) = p-1 \qquad (3.17)$$

であり，G(3,4p)は存在しない．

（証明）　法pに関して3が原始根であって，E(3,p)=p-1が偶数であり，E(3,4)=2であるから，

$$E(3,4p) = \mathrm{LCM}\{E(3,4), E(3,p)\}$$
$$= p-1 = \varphi(4p)/2$$

である．$3^g+1 \equiv 0 \pmod{4p}$,$(0<g<p-1)$なら，

$$3^g+1 \equiv 0 \pmod 4 \qquad (3.18)$$
$$\equiv 0 \pmod p$$

である．このとき，$3^{2g} \equiv 1 \pmod{4p}$であるから，E(3,4p)=p-1は $2g$ を整除し，$2g=k(p-1)$なる正整数kが存在する．このため，

$$0 < 2g = k(p-1) < 2(p-1),\ k=1,\ g=(p-1)/2$$

でなければならない．仮定により，$4 \mid (p-1)$ であるから，$g=2(p-1)/4$は偶数であり，これがE(3,4)=2の倍数であるから，$3^g \equiv 1 \pmod 4$となり，式(3.18)に反する．　（証明終）

［補題３．８］　法pに関して3でなく-3が原始根なら，

$$E(3,4p) = p-1 \qquad (3.19)$$

であり，G(3,4p)は存在しない．

（証明）　法pに関して3でなく-3が原始根であるなら，補題３．３により，E(3,p)=(p-1)/2であり，これは奇数である．このため，法A=4pに関して3が属するべき数は，

$$E(3,4p) = \mathrm{LCM}\{E(3,4), E(3,p)\}$$
$$= p-1 = \varphi(4p)/2$$

である．以下，補題３．９と同様にして，G(3,4p)が存在しないことが証明される．
（証明終）

補題３．７，３．８および定理３．２，３．６により，次の定理が導かれる．

［定理３．９］　pが5以上の素数で，生成数A=4pとする．法pに関して3が原始根であって，かつ，4がp-1を整除するなら，あるいは，法pに関して3でなく-3が原始根であるなら，

$$M_{ST}(4p,4) = (3^{p-1}-1)/(4p) \qquad (3.20)$$

である．　（証明略）

例３．４　A=4×11=44のとき，法11に関して3でなく-3が原始根であるから，式(3.20)により，

$$M_{ST}(44,4)=(3^{10}-1)/44=1342$$

である．Nを-671＜N＜671に限れば，A=44で生成されるＳＴ－ＡＮ符号の最小距離はd_m=4以上である．

最後に，生成数Aが2のべき乗で表される場合，すなわち，$A=2^{\alpha}$，($\alpha \geqq 3$)を考える．基数3は法2^1,2^2に関する原始根であるが，αが3以上の場合，3,-3はいずれも法2^{α}に関する原始根でない．法2^{α}に関する既約剰余系は，$2^{\alpha-1}$個の奇数のみからなり，その位数は$\varphi(2^{\alpha})=2^{\alpha-1}$である．

［補題３．９］　αは3以上の整数とする．法2^{α}に関して3が属するべき数は，

$$E(3,2^{\alpha}) = \varphi(2^{\alpha})/2 = 2^{\alpha-2} \qquad (3.21)$$

であり，$G(3,2^{\alpha})$は存在しない．ここで，$(3^{E(3,2^{\alpha})}-1)/2^{\alpha}$は奇数である．

（証明）　3以上のある整数kに対して，αが$3 \leqq \alpha \leqq k$であるとき，式(3.21)が成り立つと仮定する．実際，k=3の場合,すなわち，α=3のとき，$3^1 \equiv 3, 3^2=2^3 \times 1+1 \equiv 1 \pmod{2^3}$であるから，$E(3,2^3)=2$であり，$3^g \equiv -1 \pmod{2^3}$を満たすgは存在しない．また，$E(3,2^3)=2$，$(3^2-1)/2^3=1$である．$\alpha$=kのとき，上の仮定により，

$$3^{E(3,2^k)} = 3^{2^{k-2}} = 2^k q_k + 1$$

であり，

$$\begin{aligned} 3^{2E(3,2^k)} &= 3^{2^{k-1}} = (2^k q_k + 1)^2 \\ &= 2^{k+1}(2^{k-1} q_k + 1) q_k + 1 \\ &\equiv 1 \pmod{2^{k+1}} \end{aligned}$$

である．したがって，$E(3,2^{k+1})$ は $2E(3,2^k)=2^{k-1}$ を整除する． 明らかに，$E(3,2^{k+1}) \neq 2^0$ である．仮定により，

$$3^{2^1} = 2^3 q_3 + 1,\ 3^{2^2} = 2^4 q_4 + 1,\ \cdots,\ 3^{2^{k-2}} = 2^k q_k + 1$$

であり，$q_3, q_4, \cdots, q_k$ がすべて奇数である．すなわち，上式はどのひとつも法2^kに関して1と合同ではなく，$E(3,2^{k+1})$は 2^{k-2}以下でない．このため，$E(3,2^{k+1}) = 2^{k-1} = 2E(3,2^k)$ であり，$q_{k+1}=(2^{k-1} q_k + 1) q_k$ もまた奇数である． いま，$G(3,2^{k+1})$が存在すると仮定すると， 補題３．１により，$G(3,2^{k+1})=E(3,2^{k+1})/2 = 2^{k-2}$でなければならない．$3^{2^{k-2}} = 2^{k+1} q'_{k+1} - 1$なる整数$q'_{k+1}$が存在して，これに$3^{2^{k-2}} = 2^k q_k + 1$を加えて，両辺を2で割ると，

$$3^{2^{k-1}} = 2^{k-1}(2q'_{k+1} + q_k)$$

を得る．上式の左辺は奇数，右辺は偶数となり，矛盾を生じる． （証明終）

上の補題，定理３．６および定理３．２により，以下の定理を得る．

［定理３．１０］ αが3以上の整数で，生成数$A=2^\alpha$なら，

$$M_{ST}(2^\alpha, 4) = (3^{2^{\alpha-2}} - 1)/2^\alpha \qquad (3.22)$$

であって，これは奇数である． （証明略）

例３．５ $A=2^4=16$のとき，法16に関して3が属するべき数は，補題３．９により，$E(3,16)=2^2=4$である．実際，法16に関して，

$3^1 \equiv 3,\ 3^2 \equiv -7,\ 3^3 \equiv -5,\ 3^4 \equiv 1$

であり，G(3,16)は存在しない．式(3.22)により，

$M_{ST}(16,4) = (3^4-1)/2^4 = 5$

を得る．このため，情報整数Nの範囲を$-2 \leqq N \leqq 2$に限れば，A=16で生成されるＳＴ－ＡＮ符号の最小距離は4以上である．実際，

$16\times1 = (01\bar{1}\bar{1}1)_{ST}$　　$16\times4 = (1\bar{1}101)_{ST}$

$16\times2 = (011\bar{1}\bar{1})_{ST}$　　$16\times5 = (1000\bar{1})_{ST}$

$16\times3 = (1\bar{1}\bar{1}10)_{ST}$

であり，d_m=4である．

以上の定理３．８～３．１０で与えられる$M_{ST}(A,4)$の代表的な値を表３．３に示す．これに対し，電子計算機を用いて121以下の3と互いに素なすべての正整数Aについて逐次調査した．しかし，Aの値に比べて大きな$M_{ST}(A,4)$の値をもつものはこれらの定理の条件を満たすA以外には存在しなかった．

本節の最後に，電子計算機を用いて調査した$M_{ST}(A,5)$，$M_{ST}(A,6)$および$M_{ST}(A,7)$の代表的な値をそれぞれ表３．４，３．５および３．６に示す．

３．５　結　言

対称３進表現(ST表現)とST算術重みに基づく対称３進算術ＡＮ符号(ＳＴ－ＡＮ符号)の基礎理論について述べた．$M_{ST}(A,d)$は情報整数の範囲を決める重要なパラメータである．これは，D.T.Brown[3]やW.W.Peterson[36]によって２進算術ＡＮ符号に導入された概念である．さらに，T.R.N.Raoら[37]によって３進算術ＡＮ符号における同様なパラメータに関する定理を導いている．本章では，ＳＴ－ＡＮ符号における$M_{ST}(A,2)$,$M_{ST}(A,3)$および$M_{ST}(A,4)$の公式とそれらの代表的な値を示した．$M_{ST}(A,3)$の公式は，ST算術距離に基づくものであり，T.R.N.Raoらによって与えられたものと同様の方法で導かれるものである．$M_{ST}(A,4)$の公式はＳＴ－ＡＮ符号独特のものである．さらに，$M_{ST}(A,5)$,$M_{ST}(A,6)$および$M_{ST}(A,7)$を電子計

算機によって逐次調査し，その代表的な値を示した．

表３．１　法Aに関するべき数E(3,A)とG(3,A)
（A*はAが素数を意味する．）

A	E(3,A)	G(3,A)	A	E(3,A)	G(3,A)
2*	1		62	30	15
4	2	1	64	16	
5*	4	2	65	12	
7*	6	3	67*	22	11
8	2		68	16	
10	4	2	70	12	
11*	5		71*	35	
13*	3		73*	12	6
14	6	3	74	18	9
16	4		76	18	9
17*	16	8	77	30	
19*	18	9	79*	78	39
20	4		80	4	
22	5		82	8	4
23*	11		83*	41	
25	20	10	85	16	
26	3		86	42	21
28	6	3	88	10	
29*	28	14	89*	88	44
31*	30	15	91	6	
32	8		92	22	
34	16	8	94	23	
35	12		95	36	
37*	18	9	97*	48	24
38	18	9	98	42	21
40	4		100	20	
41*	8	4	101*	100	50
43*	42	21	103*	34	17
44	10		104	6	
46	11		106	52	26
47*	23		107*	53	
49	42	21	109*	27	
50	20	10	110	20	
52	6		112	12	
53*	52	36	113*	112	56
55	20		115	44	
56	6		116	28	
58	28	14	118	29	
59*	29		119	48	
61*	10	5	121	5	

表３．２　$M_{ST}(A,3)$の代表的な値

A	$M_{ST}(A,3)$	$AM_{ST}(A,3)$
5	2	3^2+1
7	4	3^3+1
11	22	3^5-1
17	386	3^8+1
19	1 036	3^9+1
23	7 702	$3^{11}-1$
29	164 930	$3^{14}+1$
31	462 868	$3^{15}+1$
43	243 264 028	$3^{21}+1$
47	2 003 046 358	$3^{23}-1$
53	47 959 732 610	$3^{26}+1$
59	1 163 226 734 998	$3^{29}-1$
71	704 669 649 281 686	$3^{35}-1$
79	51 298 166 493 911 092	$3^{39}+1$
83	439 433 691 291 214 294	$3^{41}-1$
89	11 064 841 597 568 665 538	$3^{44}+1$
101	7 107 900 868 236 164 245 250	$3^{50}+1$

表３．３　$M_{ST}(A,4)$の代表的な値

A	$M_{ST}(A,4)$	$AM_{ST}(A,4)$
$14 = 2\times7$	2	3^3+1
$16 = 2^4$	5	3^4-1
$22 = 2\times11$	11	$3^5\ \ 1$
$32 = 2^5$	205	3^8-1
$34 = 2\times17$	193	3^8+1
$38 = 2\times19$	518	3^9+1
$44 = 4\times11$	1 342	$3^{10}-1$
$46 = 2\times23$	3 851	$3^{11}\ 1$
$58 = 2\times29$	82 465	$3^{14}+1$
$62 = 2\times31$	231 434	$3^{15}+1$
$64 = 2^6$	672 605	$3^{16}-1$
$86 = 2\times43$	121 632 014	$3^{21}+1$
$92 = 4\times23$	341 098 474	$3^{22}-1$
$94 = 2\times47$	1 001 523 179	$3^{23}-1$
$106 = 2\times53$	23 979 866 305	$3^{26}+1$
$116 = 4\times29$	197 213 728 060	$3^{28}-1$
$118 = 2\times59$	581 613 367 499	$3^{29}-1$

表３．４　$M_{ST}(A,5)$の代表的な値

A	$M_{ST}(A,5)$	$AM_{ST}(A,5)$
41	2	3^4 +1
61	4	3^5 +1
97	5	3^6 -3^5 -1
143	10	3^7 -3^6 -3^3 -1
193	34	3^8 +1
259	76	3^9 +1
503	100	3^{10} -3^8 -3^7 -1
509	116	3^{10} -3^2 $+3^1$ +1
611	278	3^{11} -3^8 -3^6 +1
761	934	3^{12} $+3^{11}$ $+3^7$ -1
853	1 846	3^{13} -3^9 -3^1 +1
859	1 856	3^{13} -3^3 $+3^2$ -1
1 187	4 024	3^{14} -3^8 $+3^4$ -1
1 199	11 968	3^{15} $+3^6$ -3^1 -1

表３．５　$M_{ST}(A,6)$の代表的な値

A	$M_{ST}(A,6)$	A	$M_{ST}(A,6)$
122	2	1 208	440
142	4	1 420	499
146	5	1 436	740
302	7	1 616	992
386	17	1 900	1 585
518	38	2 138	6 739
602	44	2 692	15 859
842	70	3 064	42 149
916	191	3 596	95 618
1 126	314	3 806	305 371

表３．６　$M_{ST}(A,7)$の代表的な値

A	$M_{ST}(A,7)$	A	$M_{ST}(A,7)$
365	2	11 641	137
547	4	16 069	196
875	5	16 493	290
1 993	10	22 799	638
2 981	20	24 461	1 108
3 851	46	27 157	3 170
8 176	65	37 463	3 319
8 237	67	38 863	3 326
9 415	94	42 739	5 036
11 515	106	48 941	23 752

第４章　巡回ＳＴ－ＡＮ符号

４．１　緒　言

本章では，巡回ＳＴ－ＡＮ符号の基礎理論について述べる．この符号に対して，第２章で定義した法3^n-1に関するモジュラ距離を導入し，最小距離と誤り訂正能力の関係を示す．巡回ＳＴ－ＡＮ符号の整数論的構造に基づいて，符号語数の約数を法とする絶対最小既約剰余系の元と符号語のST算術重みとの関係を示す．

４．２　巡回ＳＴ－ＡＮ符号の構造

ＳＴ－ＡＮ符号が巡回けた移動のもとに閉じているとき，この符号を巡回ＳＴ－ＡＮ符号という．法3^n-1に関する絶対最小完全剰余系

$$Z_{AB} = \{0, \pm 1, \pm 2, \cdots, \pm(3^n-3)/2, (3^n-1)/2\} \qquad (4.1)$$

を考える．このZ_{AB}は法3^n-1に関して加算と乗算のもとに環をなす．法3^n-1を整除する任意の正整数をAとして，Z_{AB}におけるすべてのAの倍数からなる部分集合 I_A に着目する．このとき，I_A は，整数の環Z_{AB}においてAで生成されるイディアルを成す． イディアル I_A は巡回けた移動のもとに閉じている． それゆえ，I_A は巡回ＳＴ－ＡＮ符号である．言い換えれば，I_A の任意の元ANのST表現を$(a_{n-1}a_{n-2}\cdots a_0)_{ST}$とすれば，ANの1けた左巡回けた移動は

$$(a_{n-2}\cdots a_0 a_{n-1})_{ST} = AN \times 3 - a_{n-1}(3^n-1)$$

である．これはZ_{AB}の元であり，Aの倍数であるから，I_Aの元である．

巡回ＳＴ－ＡＮ符号 I_A の生成数をA，符号長をn および，符号語数をBとすると，A,B,nの間に，

$$AB = 3^n - 1 \qquad (4.2)$$

が成立する．また，情報整数Nは法Bに関する絶対最小完全剰余系Z_Bの元である．巡回ＳＴ－ＡＮ符号 I_A はZ_Bの元のA倍すべてからなる集合であり，I_Aは以下の

ように表せる．

$$I_A = A \cdot Z_B \qquad (4.3)$$

式(4.2)からも明らかなように，3とBは互いに素，すなわち，(3,B)=1である．法Bに関して3が属するべき数をE(3,B)で表すことにする．E(3,B)がnを整除するとき，そのときに限って，Bは3^n-1を整除する．すなわち，巡回ＳＴ－ＡＮ符号 I_A の符号長nはE(3,B)の倍数であり，

$$n = kE(3,B),\ (k=1,2,3,\cdots) \qquad (4.4)$$

と表すことができる．とくに，k=1のとき，この巡回ＳＴ－ＡＮ符号を基本符号といい，I_{A1}と書くことがある．また，上式のk≧2の場合の巡回ＳＴ－ＡＮ符号を繰り返し符号といい，I_{Ak}と書くことがある．繰り返し符号 I_{Ak}の生成数A_kは，

$$A_k = \frac{3^{kn_1}-1}{B}$$

$$= \frac{3^{kn_1}-1}{3^{n_1}-1}\ \frac{3^{n_1}-1}{B} = \frac{3^{kn_1}-1}{3^{n_1}-1}\ A_1$$

で与えられる．このとき，I_{Ak}の任意の符号語A_kNは

$$A_kN = \frac{3^{kn_1}-1}{3^{n_1}-1}\ A_1N$$

である．A_1Nは基本符号 I_{A1}の符号語であるから，n_1けたのST表現で表すことができる．それゆえ，A_kNのST表現すなわち繰り返し符号の符号語は基本符号 I_{A1}の符号語A_1Nをk個並べたものに一致する．

Bの約数をd_j($1 \leq d_j \leq B$)で表すことにする．法B/d_jに関する絶対最小既約剰余系$G(B/d_j)$を考える．このとき，巡回ＳＴ－ＡＮ符号 I_Aは次のように展開される．

$$I_A = \sum_{d_j|B} Ad_j \cdot G(B/d_j) \qquad (4.5)$$

I_A の部分集合 $Ad_j \cdot G(B/d_j)$は I_A の部分符号と呼ばれる．$G(B/d_j)$は法B/d_jに関する乗算のもとにアーベル群をなし，その位数はオイラー関数$\varphi(B/d_j)$で与えられる．

3^kの法B/d_jに関する絶対最小剰余を $3^k \bmod(B/d_j)$で表すことにする．任意のkに対して，3^KとB/djは互いに素であるから，$3^k \bmod(B/d_j)$は$G(B/d_j)$の元である．

それゆえ，$G(B/d_j)$の部分集合，

$$H_{(1)}(B/d_j) = \{(3^k \bmod(B/d_j)) \mid k=1,2,\cdots,E(3,B/d_j)\} \quad (4.6)$$

は，$G(B/d_j)$の巡回部分群を成す．この部分群により，$G(B/d_j)$を以下のようなコセットに展開することができる．

$$H_{(\ell)}(B/d_j) = \{(b_\ell 3^k \bmod(B/d_j)) \mid k=1,2,\cdots,E(3,B/d_j)\},$$
$$(\ell = 1,2,\cdots,\nu_j,\ b_\ell \in G(B/d_j)). \quad (4.7)$$

ここに，ν_j はコセットの個数であり，

$$\nu_j = \varphi(B/d_j)/E(3,B/d_j) \quad (4.8)$$

で与えられる．このため，部分符号$Ad_j \cdot G(B/d_j)$は，さらに，ν_j個の部分集合$Ad_j \cdot H_{(1)}(B/d_j)$に展開される．この部分集合を素符号という．各素符号はそこに含まれる符号語の任意のひとつを巡回けた移動したもので尽くされる．このことを強巡回的という．

例４．１　B=22とすると，n=E(3,22)=5，A=$(3^5-1)/22$=11である．巡回ＳＴ－ＡＮ符号 I_{11}は，

$$I_{11} = 242 \cdot G(1) + 121 \cdot G(2) + 22 \cdot G(11) + 11 \cdot G(22)$$

のように，4個の部分符号に展開される．ここに，

$G(1) = \{0\}$，

$G(2) = \{1\}$，

$G(11) = \{\pm1, \pm2, \pm3, \pm4, \pm5\}$，

$G(22) = \{\pm1, \pm3, \pm5, \pm7, \pm9\}$

であり，I_{11}の部分符号$242 \cdot G(1)$,$121 \cdot G(2)$はそれぞれ１個の符号語のみからなり，

$242 \cdot G(1) = (00000)_{ST}$，

$121 \cdot G(2) = 121 = (11111)_{ST}$

である．残りの部分符号については，$\varphi(11)=\varphi(22)=10$，$E(3,11)=E(3,22)=5$ であるから，

$G(11) = H_{(1)}(11) + H_{(2)}(11)$，

$G(22) = H_{(1)}(22) + H_{(2)}(22)$

である．ここに，

$H_{(1)}(11)=\{3,-2,5,4,1\}$, $H_{(2)}(11)=\{-3,2,-5,-4,-1\}$

$H_{(1)}(22)=\{3,9,5,-7,1\}$, $H_{(2)}(22)=\{-3,-9,-5,7,-1\}$

である．たとえば，素符号22・$H_{(1)}(11)=\{66,-44,110,88,22\}$ の各元は，

$66=(1\bar{1}110)_{ST}$, $-44=(\bar{1}1101)_{ST}$, $110=(11011\bar{1})_{ST}$, $88=(101\bar{1}1)_{ST}$, $22=(01\bar{1}11)_{ST}$

であり，これら5個の符号語は任意のひとつを巡回けた移動したもので尽くされる．

４．３　最小距離と誤り訂正能力

巡回ＳＴ－ＡＮ符号 I_A に対して，法3^n-1に関する絶対最小完全剰余系 Z_{AB} 上で定義されるモジュラST重み，モジュラST距離が用いられる．

巡回ＳＴ－ＡＮ符号 I_A の {0} 以外の符号語のモジュラST重みの最小値 w_m を I_Aの最小重みという． I_A の相異なる符号語間のモジュラST距離の最小値 d_m を I_Aの最小距離という．巡回ＳＴ－ＡＮ符号 I_A は，法3^n-1に関する整数環のイディアルであって，法3^n-1に関する加算のもとに群をなす． したがって， I_Aの任意の符号語AN_1,AN_2に対して，AN_1-AN_2も I_Aの符号語である．このため，最小距離に等しいモジュラST重みをもつ符号語が I_Aに存在し，$w_m \leqq d_m$である．最小重み w_mに等しいモジュラST重みをもつ符号語と0との間のモジュラST距離はw_mに等しく，このため，$d_m \leqq w_m$である．以上により，$w_m=d_m$を得る．すなわち，次の定理が成立する．

［定理４．１］　巡回ＳＴ－ＡＮ符号 I_Aの最小距離d_mは最小重みw_mに等しい．

（証明略）

以下，巡回ＳＴ－ＡＮ符号において取り扱う算術誤りEは，雑音や装置の障害のため，符号語ANに算術的に加えられるST表現でnけた以下の正負の整数である．受信語をVとすれば，V＝AN＋Eで与えられる．ここに，＋は法3^n-1に関する加算を意味する．

巡回ＳＴ－ＡＮ符号 I_Aの最小距離と誤り訂正能力との関係については，法3^n-

1に関するモジュラST距離の性質２．９～11から，以下の定理と系が導かれる．

［定理４．２］ 最小距離d_mが d+1 以上のとき，そのときに限って，d重以下のすべての算術誤りの検出が可能である．また，d_mが 2t+1 以上であるとき，そのときに限って，t重以下のすべての算術誤りの訂正が可能である．

（証明） 任意の符号語AN_1にd重以下の算術誤りEが生じて，

$$AN_1 + E = AN_2 \qquad (4.9)$$

を満たす符号語AN_2が存在しなければ，この算術誤りEを検出することができる．上式が成り立つと仮定すると，$AN_2 - AN_1 \equiv E \pmod{AB}$であるから，

$$d+1 \leqq D_{MST}(AN_1, AN_2) = W_{MST}(AN_2 - AN_1)$$
$$= W_{MST}(E) \leqq d$$

なる矛盾を生じる．すなわち，d重以下の算術誤りEに対して式(4.9)が成立せず，したがって，d重以下のすべての算術誤りEの検出が可能である．最小距離d_mがd以下の場合，$D_{MST}(AN_1, AN_2)=d_1 \leqq d$ なる符号語AN_1, AN_2が存在し，$E \equiv AN_2 - AN_1 \pmod{AB}$ なる算術誤りEを考えると，$W_{MST}(E)=d_1 \leqq d$である．符号語AN_1にこのようなd_1重誤りEが生ずれば，受信語はAN_2なる符号語になり，このようなd重以下の算術誤りの検出は不可能である．

任意の符号語AN_1, AN_2に対して，

$$AN_1 + E_1 = AN_2 + E_2 \qquad (4.10)$$

を満たすt重以下の算術誤りE_1, E_2が存在しなければ，そのときに限って，受信語AN_1+E_1に符号語AN_1を一意に対応させることができる．すなわち，AN_1+E_1を正しくAN_1に復号することができる．式(4.10)が成立すると仮定すると，$AN_2 - AN_1 \equiv E_1 - E_2 \pmod{AB}$ であるから，式(2.22)により，

$$2t+1 \leqq D_{MST}(AN_1, AN_2) = W_{MST}(AN_2 - AN_1)$$
$$= W_{MST}(E_1 - E_2) \leqq W_{MST}(E_1) + W_{MST}(E_2) \leqq 2t$$

なる矛盾を生じる． すなわち，d_m=2t+1 のとき，t重以下のどのような算術誤りE_1, E_2に対しても式(4.10)は成り立たず，t重以下のすべての算術誤りの訂正が可能である．最小距離d_mが2t以下の場合，

$$D_{MST}(AN_1, AN_2) = 2t_1 \text{ or } 2t_1 - 1 \leqq 2t$$

なる符号語AN_1,AN_2が存在する．このとき，

$$AN_2 - AN_1 \equiv E \pmod{AB}$$

なる算術誤りEを考えると，$W_{MST}(E)=2t_1$ or $2t_1-1 \leqq 2t$である．
EのST表現において，左からt_1個の非零けたを取り，その和を$-E_1$とし，$E_2=E+E_1$とすると，$W_{MST}(E_1)=t_1$，$W_{MST}(E_2)=t_1$ or t_1-1 である．このような算術誤りE_1，E_2に対して，式(4.10)が成り立ち，受信語$AN_1+E_1=AN_2+E_2$から一意にAN_1に復号することは不可能である．　　（証明終）

［系４．１］　最小距離d_mが t+d+1 以上のとき，t重以下のすべての算術誤りを訂正し，d(>t)重以下のすべての算術誤りを検出することが可能である．（証明略）

４．４　素符号の重み

４．２節で述べたように，l_Aは部分符号，さらに素符号へと展開される．素符号は強巡回的であるから，素符号に含まれる符号語のモジュラST重みはすべて等しい．このモジュラST重みを素符号の重みという．

l_A の符号語ANのST表現を$(a_{n-1}\cdots a_1 a_0)_{ST}$とすると，式(4.2)により，

$$a_{n-1}3^{n-1}+\cdots+a_1 3+a_0 = \frac{3^n-1}{B} N$$

である．上式の両辺を3^iで割り算して，その整数部を取り出せば，

$$B(a_{n-1}3^{n-1-i}+\cdots+a_i) = N3^{n-i}-(N3^{n-i}) \bmod B$$

となる．このとき，

$$a_i B \equiv -(N3^{n-i}) \bmod B \pmod 3$$

である．(3,B)=1であるから，B mod 3 は1または-1である．したがって，

$$a_i = -(B \bmod 3)[((N3^{n-i}) \bmod B) \bmod 3],$$

$$(i=0,1,2,\cdots,n-1) \qquad (4.11)$$

である．a_iが零か非零かは，$(N3^{n-i}) \bmod B$ が3の倍数か否かによる．それゆえ，符号語ANのモジュラST重みは，iが 0からn-1までを変わるとき，$(N3^{n-i}) \bmod B$ のうち3の倍数でないものの個数に等しい．いま，ANが素符号$Ad_j \cdot H_{\phi}(B/d_j)$に属し

ており，式(4.7)においてk=E(3,B/d_j)とする．このとき，AN=A$d_j b_\ell$で表される．Bの約数d_jは3と互いに素であるから，

$$(N3^{n-i}) \bmod B = (d_j b_\ell 3^{n-i}) \bmod B$$
$$= d_j[(b_\ell 3^{n-i}) \bmod (B/d_j)]$$

である．iが0からn-1までを変わるとき，$[(b_\ell 3^{n-i}) \bmod (B/d_j)]$は$H_{(\omega)}(B/d_j)$の元を丁度 n／E(3,B/$d_j$)回変わる．以上により，次の定理が成立する．

［定理４．３］ 素符号Ad_j・$H_{(\omega)}(B/d_j)$の重みwは

$$w = W_{MST}(Ad_j b_\ell) = \frac{n}{E(3,B/d_j)} \times \#\{e \mid e \in H_{(\omega)}(B/d_j),\ (3,e)=1\} \quad (4.12)$$

ここに，#{Ｓ}は集合Ｓの要素数を表す．　（証明略）

巡回ＳＴ－ＡＮ符号の最小距離は，I_nを構成する {0} 以外の素符号の重みを定理４．３により算定し，それらの最小値で与えられる．次章では，符号語数Bが特別な条件を満たす正整数のとき，その条件の範囲内で一般的にI_nの最小距離を算定する公式を導く．

第５章　巡回ＳＴ－ＡＮ符号の最小距離

５．１　緒　言

前章で述べた巡回ＳＴ－ＡＮ符号の最小距離を求めることは重要な問題である．はじめに，巡回ＳＴ－ＡＮ符号の構造を利用して，最小距離を求める一般的な方法を示す．この方法に基づき，特別な構造をもつ符号の最小距離を算定する公式を導く．最後に，その公式が得られた符号の全体的な特徴を述べる．

５．２　最小距離の算定

以下では，3と互いに素な正整数Bを符号語数として法Bに関して3が属するべき数E(3,B)によって，符号長nと生成数Aが，

$$n=E(3,B),\ A=(3^n-1)/B \qquad (5.1)$$

で与えられる巡回ＳＴ－ＡＮ符号 I_A を考える．このような I_A を符号語数Bで規定される符号という．

巡回ＳＴ－ＡＮ符号 I_A の最小距離 d_m は，以下の手順で組織的に算定することができる．

(1)　I_A の符号語数Bを素因数分解する．Bのすべての約数 d_j $(1 \leqq d_j \leqq B)$ に対応して，法 B/d_j に関する絶対最小既約剰余系 $G(B/d_j)$ を求める．

(2)　$G(1)=\{0\}$ 以外の各 $G(B/d_j)$ に対して，その巡回部分群 $H_{(1)}(B/d_j)$ により，コセット $H_{(\omega)}(B/d_j)$ に展開する．

(3)　さらに，各コセット $H_{(\omega)}(B/d_j)$ に対応する素符号 $Ad_j \cdot H_{(\omega)}(B/d_j)$ の重みを定理４．３により算定し，それらの最小値を求める．

符号語数Bが比較的小さい場合には，符号語ひとつひとつのST重み $W_{ST}(A)$, $W_{ST}(2A), W_{ST}(3A), \cdots$ を求め，その最小値を見いだすというやり方が得策であろう．しかし，Bが大きい場合には，明らかに，先に述べた手順の方が能率的である．とくに，I_A に含まれる素符号の個数が少ない場合その効果は大きいと考えられる．

p,qを5以上の素数とするとき，符号語数Bの素因数に 2,p,qを含む以下の場合について，I_A の最小距離を算定する公式を導く．

① B=p, 2p, 4p

② $B=p^{\alpha}$, $2p^{\alpha}$, $4p^{\alpha}$, $(\alpha \geqq 2)$

③ $B=2^{\gamma}$, $(\gamma \geqq 3)$

④ B=pq, 2pq

⑤ $B=p^{\alpha}q$, $2p^{\alpha}q$, $(\alpha \geqq 2)$

⑥ $B=p^{\alpha}q^{\beta}$, $2p^{\alpha}q^{\beta}$, $(\alpha, \beta \geqq 2)$

5．3　符号語数B=p, 2p, 4p で規定される符号

(a)　B=p

pは5以上の素数である．Bの約数は1とB自身である．B=pで規定される巡回ＳＴ－ＡＮ符号 I_A は，

$$I_A = A\cdot G(p) + A\cdot G(1),$$

$$(G(1)=\{0\},\ G(p)=\{\pm q \mid 1,2,\cdots,(p-1)/2\}) \qquad (5.2)$$

で表される．　すなわち，I_A は部分符号$A\cdot G(p)$とnけたすべてが0の符号語$(00\cdots0)_{ST}$ から成る．以下では，法pに関して3または-3が原始根の場合を検討する．

法pに関して3が原始根であるとき，B=pで規定される I_A は，式(5.1)により，

$$n = E(3,p) = \varphi(p) = p-1,\ A = (3^n-1)/p \qquad (5.3)$$

である．

［定理５．１］　法pに関して3が原始根のとき，B=pで規定される符号 I_A の最小距離は，

$$d_m = \begin{cases} 2(p-1)/3, & (p \equiv 1 \pmod 3) \\ 2(p+1)/3, & (p \equiv -1 \pmod 3) \end{cases} \qquad (5.4)$$

である．

（証明）　3が法pに関する原始根であるから，法pに関する絶対最小既約剰余系G(p)は，

$$G(p) = H_{(1)}(p)$$
$$= \{3^k \bmod p \mid k=1,2,\cdots,p-1\}$$

となり，１個の巡回部分群$H_{(1)}(p)=G(p)$からなる．また，pは素数であるから，式(5.2)により，

$$H_{(1)}(p) = \{\pm q \mid q=1,2,\cdots,(p-1)/2\}$$

である．したがって，素符号$A\cdot H_{(1)}(p)$の重みは，定理４．３により，

$$w = \#\{e \mid e \in G(p), (e,3)=1\}$$

である．ここで，素数pは法3に関して$p \equiv 1$ or -1 であるから，それぞれの場合に対して，式(5.4)を得る．　（証明終）

上の定理の条件を満たすB=pで規定される巡回ＳＴ－ＡＮ符号 I_A は，一つの符号語（例えばA）を巡回けた移動することにより，0以外のすべての符号語を尽くすことができる強巡回的な符号であり，等距離符号である．

法pに関して3でなく-3が原始根であるとき，B=pで規定される I_A は，補題３．３と式(5.1)により，

$$n = E(3,p) = \varphi(p)/2 = (p-1)/2, \quad A = (3^n-1)/p \qquad (5.5)$$

である．

［補題５．１］　pは5以上の素数とする．-3が法pに関して原始根なら，$p \equiv 1 \pmod 3$ではあり得ない．

（証明）　付録参照

法pに関して-3が原始根なら，(p,3)=1であるから，法3に関してp≡1でなければ，p≡-1に限られる．

[定理５．２]　法pに関して3でなく-3が原始根のとき，B=pで規定される符号 I_A の最小距離は，

$$d_m = (p+1)/3 \qquad (5.6)$$

である．

（証明）　法pに関して3でなく-3が原始根なら，補題３．３により，E(3,p)=(p-1)/2で奇数である．したがって，G(p)は2個のコセットに展開され，巡回部分群 $H_{(1)}(p)$ に-1は含まれないから，

$$G(p) = H_{(1)}(p) + H_{(2)}(p)$$
$$= \{3^k \bmod p \mid k=1,2,\cdots,(p-1)/2\}$$
$$+ \{(-1)3^k \bmod p \mid k=1,2,\cdots,(p-1)/2\}$$

である．それゆえ，G(p)の元（式(5.1)）のうち，3の倍数でないものの個数が $H_{(1)}(p)$ と $H_{(2)}(p)$ に等しく配分される．さらに，補題５．１により，p≡-1 (mod 3)の場合のみを考えれば，式(5.6)を得る．　（証明終）

上の定理の条件を満たす巡回ＳＴ－ＡＮ符号 I_A は，二つの符号語Aと-Aをそれぞれ巡回けた移動することにより，{0} 以外のすべての符号語を尽くすことができる．しかも，$W_{MST}(A)=W_{MST}(-A)$であるから，I_A は等距離符号である．

(b)　B=2p

2pの約数は1,2,p および,2p(=B)である．B=2pで規定される巡回ＳＴ－ＡＮ符号 I_A は，

$$I_A = A\cdot G(2p) + A2\cdot G(p) + Ap\cdot G(2) + A2p\cdot G(1),$$
$$(G(1)=\{0\},\ G(2)=\{1\}) \qquad (5.7)$$

のように４個の部分符号に展開される．上式の第３項，第４項については，A2p･

$G(1)=(00\cdots0)_{ST}$であり，また，$Ap\cdot G(2)=(3^n-1)/2=(11\cdots1)_{ST}$である．$G(2p)$の位数$\varphi(2p)$は，$\varphi(2p)=\varphi(p)=p-1$である．以下では，法pに関して3または-3が原始根の場合を検討する．

法pに関して3が原始根であるとき，補題３．４により，3は法2pに関しても原始根である．B=2pで規定される符号 I_A の符号長と生成数は，

$$n = E(3.2p) = \varphi(2p) = p-1,\ A = (3^n-1)/(2p) \qquad (5.8)$$

である．

［定理５．３］ 法pに関して3が原始根のとき，B=2pで規定される符号 I_A の最小距離は，

$$d_m = \begin{cases} 2(p-1)/3, & (p\equiv 1 \pmod 3) \\ 2(p-2)/3, & (p\equiv -1 \pmod 3) \end{cases} \qquad (5.9)$$

である．

（証明） 法pに関して3が原始根なら，3は法2pに関して原始根であるから，

$$G(2p) = H_{(1)}(2p) = \{3^k \bmod 2p \mid k=1,2,\cdots,p-1\}$$

である．また，$G(2p)$は，集合

$$S_1 = \{\pm q \mid q=1,2,\cdots,p-1\}$$

から2の倍数の集合

$$S_2 = \{\pm 2q \mid q=1,2,\cdots,(p-1)/2\}$$

を除いたものである．S_1，S_2の元の3の倍数でないものの個数をそれぞれw_1,w_2とすると，素符号$A\cdot H_{(1)}(2p)$の重みはw_1-w_2で与えられる．$p\equiv 1 \pmod 3$のとき，

$$w = w_1-w_2 = 4(p-1)/3 - 2(p-1)/3 = 2(p-1)/3 \qquad (5.10)$$

であり，$p\equiv -1 \pmod 3$のとき，

$$w = 2(2p-1)/3 - 2(p+1)/3 = 2(p-2)/3 \qquad (5.11)$$

である．

法pに関して3が原始根であるから，$G(p)=H_{(1)}(p)$である．したがって，これに対応する素符号$A2\cdot H_{(1)}(p)$の重みは定理５．１における素符号の重みに一致する．

すなわち，

$$w = \begin{cases} 2(p-1)/3, & (p \equiv 1 \pmod 3) \quad (5.12) \\ 2(p+1)/3, & (p \equiv -1 \pmod 3) \quad (5.13) \end{cases}$$

である．

最後に，G(2)については，$Ap \cdot G(2) = Ap = (3^n-1)/2 = (11\cdots1)_{ST}$であるから，nけたすべてが1の符号語ApのST重みは

$$w = n = p-1 \quad (5.14)$$

である．

以上により，$p \equiv 1 \pmod 3$のとき，式(5.10),(5.12),(5.14)から，それらの最小値は式(5.10)または(5.12)により与えられる．また，$p \equiv -1 \pmod 3$のとき，式(5.11),(5.13),(5.14)から，それらの最小値は式(5.11)により与えられる．

（証明終）

法pに関して3でなく-3が原始根であるとき，B=2pで規定される I_Δ の符号長nおよび生成数Aは，補題３．３，３．４と式(5.1)により，

$$n = E(3,2p) = \varphi(2p)/2 = (p-1)/2, \quad A = (3^n-1)/2p \quad (5.15)$$

である．

［定理５．４］　法pに関して3でなく-3が原始根のとき，B=2pで規定される符号 I_Δ の最小距離は，

$$d_m = (p-2)/3 \quad (5.16)$$

である．

（証明）　法pに関して3でなく-3が原始根なら，法2pに関しても3でなく-3が原始根である．このため，$E(3,2p) = \varphi(2p)/2$であり，G(2p)は2個のコセットに展開される．このとき，E(3,2p)は奇数であり，G(2p)の元-1は$H_{(1)}(2p)$には含まれない．したがって，

$$G(2p) = H_{(1)}(2p) + H_{(2)}(2p)$$
$$= \{3^k \bmod 2p \mid k=1,2,\cdots,(p-1)/2\}$$
$$+ \{(-1)3^k \bmod 2p \mid k=1,2,\cdots,(p-1)/2\}$$

である．また，G(2p)は，集合

$$S_1 = \{\pm q \mid q=1,2,\cdots,p-1\}$$

から2の倍数の集合

$$S_2 = \{\pm 2q \mid q=1,2,\cdots,(p-1)/2\}$$

を除いたものである．S_1，S_2の元の3の倍数でないものの個数をそれぞれw_1,w_2とする．素符号$A\cdot H_{(1)}(2p)$と$A\cdot H_{(2)}(2p)$の重みwは共に$(w_1-w_2)/2$で与えられる．補題５．１により，$p\equiv -1 \pmod 3$の場合のみを考える．

$$w = (w_1-w_2)/2$$
$$= (2p-1)/3 - (p+1)/3 = (p-2)/3 \qquad (5.17)$$

である．

法pに関して3でなく-3が原始根であるから，$G(p)=H_{(1)}(p)+H_{(2)}(p)$である．したがって，これに対応する素符号$A2\cdot H_{(1)}(p)$，$A2\cdot H_{(2)}(p)$の重みは定理５．２における素符号の重みに一致する．すなわち，

$$w = (p+1)/3 \qquad (5.18)$$

である．

最後に，G(2)については，

$$w = n = (p-1)/2 \qquad (5.19)$$

である．

以上により，式(5.17),(5.18),(5.19)から，それらの最小値は式(5.17)により与えられる．　　（証明終）

(c)　B=4p

4pの約数は1,2,4,p,2p,および4p(=B)である．B=4pで規定される巡回ＳＴ－ＡＮ符号 I_B は，

$$I_B = A\cdot G(4p) + A2\cdot G(2p) + A4\cdot G(p)$$
$$+ Ap\cdot G(4) + A2p\cdot G(2) + A4p\cdot G(1),$$
$$(G(1)=\{0\},\ G(2)=\{1\},\ G(4)=\{\pm 1\}) \qquad (5.20)$$

のように６個の部分符号に展開される．G(4p)の位数$\varphi(4p)$は，

$$\varphi(4p)=2(p-1) \qquad (5.21)$$

である．以下では，法pに関して3または-3が原始根の場合を検討するが，いずれ

にしても法4pに関する原始根は存在しない．

［補題５．２］ 5以上の素数pに対して，±3がともに法pの原始根なら，4 |(p-1)である．3(または-3)が法pの原始根であり，4 |(p-1)なら，-3(または3)も法pに関する原始根である．

（証明） 付録参照

法pに関して3が原始根であって，4 |(p-1)なら，補題５．２により，法pに関して-3も原始根であるから，このような p は p≡1(mod 3)に限る．また，法pに関して3が原始根であって，4 |(p-1)なら，補題３．７により，E(3,4p)＝p-1であり，

$$n = E(3,4p) = p-1 = \varphi(4p)/2 \ , \ A = (3^n-1)/(4p) \quad (5.22)$$

である．

［定理５．５］ 法pに関して3が原始根であって，かつ，4 |(p-1)なら，B=4pで規定される符号 l_A の最小距離は，

$$d_m = 2(p-2)/3 \quad (5.23)$$

である．

（証明） 最初に，G(4p)を考える．式(5.21),(5.22)により，G(4p)は2個のコセットに展開される．このとき，補題３．７により，G(4p)の元-1は$H_{(1)}(4p)$には含まれない．したがって，

$$G(4p) = H_{(1)}(4p) + H_{(2)}(4p)$$
$$= \{3^k \bmod 4p \mid k=1,2,\cdots,p-1\}$$
$$+ \{(-1)3^k \bmod 4p \mid k=1,2,\cdots,p-1\}$$

である．また，G(4p)は，集合

$$S_1 = \{\pm q \mid q=1,2,\cdots,2(p-1)\}$$

から2の倍数の集合

$$S_2 = \{\pm 2q \mid q=1,2,\cdots,p-1\}$$

とpの倍数からなる集合

$S_3 = \{\pm p\}$

を除いたものである．S_1，S_2の元の3の倍数でないものの個数をそれぞれw_1,w_2とする．素符号$A\cdot H_{(1)}(4p)$と$A\cdot H_{(2)}(4p)$の重みは共に$(w_1-w_2-2))/2$で与えられる．補題５．２により，法pに関して-3もまた原始根であるから，補題５．１により，$p\equiv -1 \pmod 3$の場合のみを考える．

$$w = (w_1-w_2-2)/2$$
$$= (4(2p-1)/3-2(2p-1)/3-2)/2$$
$$= 2(p-2)/3 \qquad (5.24)$$

である．

法pに関して3が原始根なら，3は法2pに関して原始根であるから，

$$G(2p) = H_{(1)}(2p)$$
$$= \{3^k \bmod 2p \mid k=1,2,\cdots,p-1\}$$

であり，これは，定理５．３の証明で述べたG(2p)である．ただし，法pに関して-3もまた原始根であるから，素符号$A2\cdot H_{(1)}(2p)$の重みwは $p\equiv -1 \pmod 3$の場合を考えればよく，式(5.11)により，

$$w = 2(p-2)/3 \qquad (5.25)$$

である．

法pに関して3が原始根であるから，$G(p)=H_{(1)}(p)$である．したがって，これに対応する素符号$A4\cdot H_{(1)}(p)$の重みwは定理５．１における素符号の重みのうち，式(5.3)の$p\equiv -1 \pmod 3$の場合に一致して，

$$w = 2(p+1)/3 \qquad (5.26)$$

である．

$G(4)$に対応する部分符号$Ap\cdot G(4)=\{\pm Ap\}$は$Ap=(3^n-1)/4=(1\bar{1}1\bar{1}\cdots 1\bar{1})_{ST}$と$-Ap=(\bar{1}1\bar{1}1\cdots\cdots\bar{1}1)_{ST}$との2個の符号語からなり，この符号語のST重みwは，

$$w = p-1 \qquad (5.27)$$

である．

最後に，G(2)に関しては，1個の符号語 $A2p=(11\cdots 1)_{ST}$ に対応して，このST重みは式(5.27)に等しい．

以上により，式(5.24)～(5.27)の最小値は式(5.24)または式(5.25)で与えられ

る．　　（証明終）

法pに関して3でなく-3が原始根であるとき，E(3,p)＝E(3,2p)＝(p-1)／2であり，これは奇数である．また，補題５．１により，このようなpは p≡1(mod 3)に限る．また，補題３．８の証明において，E(3,4p)＝p-1であるから，

$$n = E(3,4p) = p-1 = \varphi(4p)/2 \ , \ A = (3^n-1)/(4p) \quad (5.28)$$

である．

［定理５．６］ 法pに関して3でなく-3が原始根であるなら，B=4pで規定される符号 I_A の最小距離は，

$$d_m = 2(p-2)/3 \quad (5.29)$$

である．

（証明） 最初に，G(4p)を考える．式(5.28)により，G(4p)は2個のコセットに展開される．このとき，補題３．８により，G(4p)の元-1は$H_{(1)}(4p)$には含まれない．したがって，定理５．５の証明と同様にして，

$$G(4p) = H_{(1)}(4p) + H_{(2)}(4p)$$
$$= \{3^k \bmod 4p \mid k=1,2,\cdots,p-1\}$$
$$+ \{(-1)3^k \bmod 4p \mid k=1,2,\cdots,p-1\}$$

である．法pに関して-3が原始根であるから，補題５．１により，p≡-1 (mod 3)の場合のみを考える．

$$w = 2(p-2)/3 \quad (5.30)$$

である．

法pに関して3でなく-3が原始根なら，法2pに関して3でなく-3が原始根であるから，E(3,2p)＝φ(2p)／2により，G(2p)は2個のコセットに展開される．このとき，E(3,2p)は奇数であり，G(2p)の元-1は$H_{(1)}(2p)$には含まれない．したがって，定理５．４の証明と同様にして，

$$G(2p) = H_{(1)}(2p) + H_{(2)}(2p)$$
$$= \{3^k \bmod 2p \mid k=1,2,\cdots,p-1\}$$
$$+ \{(-1)3^k \bmod 2p \mid k=1,2,\cdots,p-1\}$$

である．この素符号A2・$H_{(1)}(2p)$は，定理５．４のB=2pで規定される符号 l_A の素符号A・$H_{(1)}(2p)$，(A=($3^{E(3,2p)}$-1)／2p) の符号語をE(3,4p)／E(3,2p)=2回繰り返した符号語で構成される．もう一つの素符号A2・$H_{(2)}(2p)$も同様であり，両素符号の重みwは，式(5.17)により，

$$w = 2(p-2)/3 \qquad (5.31)$$

である．

法pに関して3でなく-3が原始根であるから，$G(p)=H_{(1)}(p)+H_{(2)}(p)$である．したがって，これに対応する素符号A4・$H_{(1)}(p)$，A4・$H_{(2)}(p)$の重みwは相等しく，この素符号は，定理５．２における素符号の符号語をE(3,4p)／E(3,p)=2回繰り返した符号語からなる．したがって，両素符号の重みwは，式(5.6)により，

$$w = 2(p+1)/3 \qquad (5.32)$$

である．

最後に，G(4)に対応する部分符号Ap・G(4)={±Ap}および，G(2)に関しては定理５．５の場合と同様であり，これらに対応する符号語のST重みwは，

$$w = p-1 \qquad (5.33)$$

である．以上により，式(5.30)～(5.33)の最小値は式(5.30)または式(5.31)で与えられる．　（証明終）

以上，法pに関して3が原始根である場合の符号語数B=p,2p,4pで規定される符号 l_A の最小距離の算定公式をそれぞれ，定理５．１，５．３，５．５で導いた．これらの実際の符号例については表５．１に示す．また，法pに関して3でなく-3が原始根である場合の符号語数B=p,2p,4pで規定される符号 l_A の最小距離の算定公式をそれぞれ，定理５．２，５．４，５．６で導いた．これらの符号例は表５．２に示す．

５．４　符号語数$B=p^{\alpha}$，$2p^{\alpha}$，$4p^{\alpha}$ で規定される符号

(d)　$B=p^{\alpha}$

pは5以上の整数であり，αは2以上の整数である．法$B=p^{\alpha}$に関する既約剰余系

$G(p^{\alpha})$の位数は

$$\varphi(p^{\alpha}) = p^{\alpha} - p^{\alpha-1} = p^{\alpha-1}(p-1) \tag{5.34}$$

で与えられる．p^{α}の約数は $1,p,p^2,\cdots,p^{\alpha}$ であるから，このようなBで規定される符号 I_A は，

$$I_A = A\cdot G(p^{\alpha}) + Ap\cdot G(p^{\alpha-1}) + \cdots + Ap^{\alpha}\cdot G(1), \quad (G(1)=\{0\}) \tag{5.35}$$

のように，$(\alpha+1)$個の部分符号に展開される．

法p^{α}に関して3が原始根であるとき，法pに関して3が属するべき数が$E(3,p)=\varphi(p)$であるから，

$$n = p^{\alpha}-p^{\alpha-1},\ A = (3^n-1)/p^{\alpha} \tag{5.36}$$

である．

［補題５．３］ pは5以上の素数，αは2以上の整数とする．法p^{α}に関して3(または-3)が原始根なら，3(または-3)は法$p^{\alpha-1}$，$p^{\alpha-2}$，$\cdots$，p に関しても原始根である．

（証明） 付録参照

［定理５．７］ 法p^{α}に関して3が原始根なら，$B=p^{\alpha}$で規定される符号 I_A の最小距離は

$$d_m = \begin{cases} 2(p^{\alpha}-p^{\alpha-1})/3, & (p\equiv 1 (\mathrm{mod}\ 3)), \\ 2(p^{\alpha}-p^{\alpha\ 1}-2p^{\alpha-2})/3, & (p\equiv -1 (\mathrm{mod}\ 3)) \end{cases} \tag{5.37}$$

である．

（証明） 補題５．３により，式(5.35)の部分符号$Ap^{i}\cdot G(p^{\alpha-i}),(i=0,1,\cdots,\alpha-1)$はすべて強巡回的な素符号である．すなわち，法$p^i$に関する絶対最小既約剰

余系は

$$G(p^{\alpha-i}) = H_{(1)}(p^i)$$
$$= \{3^k \bmod p^i \mid k=1,2,\cdots,p^{\alpha-i}-p^{\alpha-i-1}\}$$

である．素符号$Ap^i \cdot H_{(1)}(p^i)$の重み$w(i)$は，

$$w(i) = p^i \times \#\{e \mid e \in G(p^{\alpha-i}),\ (e,3)=1\}$$

である． $G(p^{\alpha-i})$は，集合

$$S_1 = \{\pm q \mid q=1,2,\cdots,(p^{\alpha-i}-1)/2\}$$

からpの倍数の集合

$$S_2 = \{\pm pj \mid j=1,2,\cdots,(p^{\alpha-i-1}-1)/2\}$$

を除いたものである．この素符号の重み$w(i)$は，S_1,S_2のそれぞれから3の倍数を除き，残された元の個数をそれぞれw_1,w_2とすれば，

$$w(i) = p_i(w_1 - w_2)$$

で与えられる．

$$w_1 = \begin{cases} 2(p^{\alpha-i}-1)/3, & (p^{\alpha-i} \equiv 1 \pmod 3) \\ 2(p^{\alpha-i}+1)/3, & (p^{\alpha-i} \equiv -1 \pmod 3) \end{cases}$$

$$w_2 = \begin{cases} 2(p^{\alpha\ i-1}-1)/3, & (p^{\alpha-i} \equiv 1 \pmod 3) \\ 2(p^{\alpha-i-1}+1)/3, & (p^{\alpha-i} \equiv -1 \pmod 3) \end{cases}$$

であるから，

$$w(i) = \begin{cases} 2(p^{\alpha}-p^{\alpha-1})/3, & (p \equiv 1 \pmod 3) \\ 2(p^{\alpha}-p^{\alpha-1}-2p^i)/3, & (p \equiv -1 \pmod 3,\ \alpha-i \equiv 0 \pmod 2) \\ 2(p^{\alpha}-p^{\alpha-1}+2p^i)/3, & (p \equiv -1 \pmod 3,\ \alpha-i \equiv 1 \pmod 2) \end{cases} \quad (5.38)$$

である．$p \equiv 1 \pmod 3$ のとき，{0}以外のすべての素符号の重みはiに関係なくαによってのみ定まる．$p \equiv -1 \pmod 3$ のとき，$i=\alpha-2$の素符号$Ap^{\alpha-2} \cdot G(p^2)$の重みが最小となる． （証明終）

上の定理の証明により，法p^{α}に関して3が原始根であるとき，$p \equiv 1 \pmod 3$ なら，$B=p^{\alpha}$で規定される符号 l_A は等距離符号である．

法p^{α}に関して3でなく-3が原始根である場合，補題３．３により，$E(3,p^{\alpha}) =$

$\varphi(p^{\alpha})/2=(p^{\alpha}-p^{\alpha-1})/2$であるから，

$$n = p^{\alpha}-p^{\alpha-1})/2,\ A = (3^n-1)/p^{\alpha} \qquad (5.39)$$

である．

［補題５．４］ pは5以上の素数，αは2以上の整数とする．法p^{α}に関して3でなく-3が原始根なら，法$p^{\alpha-i}$に関して3が属するべき数は，

$$E(3,p^{\alpha-i}) = \varphi(p^{\alpha-i})/2.\ (i=0,1,\cdots,\alpha-1) \qquad (5.40)$$

であり，これは奇数である．

（証明）　付録参照．

［定理５．８］ 法pに関して3でなく-3が原始根なら，$B=p^{\alpha}$で規定される符号 l_A の最小距離は，

$$d_m = (p^{\alpha}-p^{\alpha-1}-2p^{\alpha-2})/3 \qquad (5.41)$$

（証明）　補題５．４により，絶対最小既約剰余系$G(p^{\alpha-i})$は，

$$G(p^{\alpha-i}) = H_{(1)}(p^{\alpha-i}) + H_{(2)}(p^{\alpha-i}),$$

$$H_{(1)}(p^{\alpha-i}) = \{3^k \bmod p^{\alpha-i} \mid k=1,2,\cdots,p^{\alpha-i-1}(p-1)/2\} \qquad (5.42)$$

のように，２個のコセットに展開される．$E(3,p^{\alpha-i})$が奇数であるから，$G(p^{\alpha-i})$の元 -1 は，$H_{(1)}(p^{\alpha-i})$に含まれず，$H_{(2)}(p^{\alpha-i})$に含まれる．このため，

$$H_{(2)}(p^{\alpha-i}) = \{(-1)3^k \bmod p^{\alpha-i} \mid k=1,2,\cdots,p^{\alpha-i-1}(p-1)/2\}$$
$$= -1\cdot H_{(1)}(p^{\alpha-i})$$

である．それゆえ，$G(p^{\alpha-i})$の元のうち，3の倍数でないものが双方のコセットに等しく配分される．補題５．３により，-3が法pに関して原始根であるから，補題５．１により，$p\equiv -1 \pmod 3$の場合のみを考える．定理５．７の証明の後半で得られる結果を利用して，$p\equiv -1 \pmod 3$の場合，素符号$Ap^{\alpha-2}\cdot H_{(1)}(p^2)$，または，$Ap^{\alpha-2}\cdot H_{(2)}(p^2)$の重みが最小であり，式(5.41)を得る．　　（証明終）

(e)　$B=2p^{\alpha}$

法$B=2p^{\alpha}$に関する既約剰余系$G(2p^{\alpha})$の位数は，

$$\varphi(2p^{\alpha}) = p^{\alpha} - p^{\alpha-1} \qquad (5.43)$$

である．$B=2p^{\alpha}$の約数が $1,p,p^2,\cdots,p^{\alpha},2,2p,2p^2,\cdots,2p^{\alpha}$であるから，このような符号語数Bで規定される符号 I_B は，

$$I_B = A\cdot G(2p^{\alpha}) + Ap\cdot G(2p^{\alpha-1}) + \cdots + Ap^{\alpha}\cdot G(2)$$
$$+ A2\cdot G(p^{\alpha}) + A2p\cdot G(p^{\alpha-1}) + \cdots + A2p^{\alpha}\cdot G(1),$$
$$(G(1)=\{0\},\ G(2)=\{1\}) \qquad (5.44)$$

のように，$2(\alpha+1)$個の部分符号に展開される．

法p^{α}に関して3が原始根である場合を考える．

［補題５．５］　法p^{α}に関して3（または-3）が原始根であるとき，そのときに限って，3（または-3）は法$2p^{\alpha}$が原始根である．さらにこのとき，3（または-3）は法$2p^{\alpha-1},2p^{\alpha-2},\cdots,2p$に関する原始根である．

（証明）　付録参照

上の補題により，3が法$2p^{\alpha}$に関する原始根であるから，

$$n = p^{\alpha} - p^{\alpha-1},\ A = (3^{n}-1)/(2p^{\alpha}) \tag{5.45}$$

である．

［定理５．９］　法p^{α}に関して3が原始根なら，$B=2p^{\alpha}$で規定される符号 l_A の最小距離は

$$d_m = \begin{cases} 2(p^{\alpha} - p^{\alpha-1})/3, & (p \equiv 1 \pmod 3), \\ 2(p^{\alpha} - 2p^{\alpha-1})/3, & (p \equiv -1 \pmod 3) \end{cases} \tag{5.46}$$

である．

（証明）　補題５．３，５．５により，3が法$p^{\alpha-i}$,法$2p^{\alpha-i}$,$(i=0,1,\cdots,\alpha-1)$の原始根であるから，式(5.43)の部分符号$Ap^{i}\cdot G(2p^{\alpha-i})$,$A2p^{i}\cdot G(p^{\alpha-i})$はすべて強巡回的な素符号である．はじめに，素符号$Ap^{i}\cdot G(2p^{\alpha-i})$を考える．$n=p^{\alpha}-p^{\alpha-1}$が$E(3,2p^{\alpha-i})=p^{\alpha-i}-p^{\alpha-i-1}$の$p^{i}$倍であるから，この素符号の重みw(i)は，

$$w(i) = p^{i} \times \#\{e \mid e \in G(2p^{\alpha-i}),\ (3,e)=1\}$$

である．$G(2p^{\alpha-i})$は，集合

$$S_1 = \{\pm q \mid q=1,2,\cdots,p^{\alpha-i-1}\}$$

から，2の倍数の集合

$$S_2 = \{\pm 2j \mid j=1,2,\cdots,(p^{\alpha-i}-1)/2\}$$

とpの倍数の集合

$$S_3 = \{\pm pj \mid j=1,2,\cdots,p^{\alpha-i-1}\}$$

を除き，2pの倍数の集合

$$S_4 = \{\pm 2pj \mid j=1,2,\cdots,(p^{\alpha-i-1}-1)/2\}$$

を加えて補正したものである．さらに，これら（S_1～S_4）の元のうち，それぞれから3の倍数を除いて，

$$w(i) = \begin{cases} 2(p^{\alpha}-p^{\alpha-1})/3, & (p\equiv 1(\mathrm{mod}\ 3), \\ 2(p^{\alpha}-p^{\alpha-1}+p^{i})/3, & (p\equiv -1(\mathrm{mod}\ 3), \alpha-i\equiv 0(\mathrm{mod}\ 2)), \\ 2(p^{\alpha}-p^{\alpha-1}-p^{i})/3, & (p\equiv -1(\mathrm{mod}\ 3), \alpha-i\equiv 1(\mathrm{mod}\ 2)) \end{cases} \tag{5.47}$$

を得る．$p\equiv -1(\mathrm{mod}\ 3)$の場合，$i=\alpha-1$のとき，$w(i)$が最小になる．すなわち，$Ap^{i}\cdot G(2p^{\alpha-i}),(i=0,1,\cdots,\alpha-1)$の素符号のうち，最小の重みを与えるものは$Ap^{\alpha-1}\cdot G(2p^{i})$であり，その重み$w(\alpha-1)$は，

$$w(\alpha-1) = \begin{cases} 2(p^{\alpha}-p^{\alpha-1})/3, & (p\equiv 1(\mathrm{mod}\ 3), \\ 2(p^{\alpha}-2p^{\alpha-1})/3, & (p\equiv -1(\mathrm{mod}\ 3)) \end{cases} \tag{5.48}$$

である．次に，素符号$A2p^{i}\cdot G(p^{\alpha-i})$を考える．これらは定理５．７で示した素符号$Ap^{i}\cdot G(p^{\alpha-i})$に一致する．これらの素符号の重み$w(i)$は式(5.38)で与えられ，最小重みを与える素符号は$i=\alpha-2$の場合であり，

$$w(\alpha-2) = \begin{cases} 2(p^{\alpha}-p^{\alpha-1})/3, & (p\equiv 1(\mathrm{mod}\ 3)), \\ 2(p^{\alpha}-p^{\alpha-1}-2p^{\alpha-2})/3, & (p\equiv -1(\mathrm{mod}\ 3)) \end{cases} \tag{5.49}$$

である．最後に，素符号$Ap^{\alpha}\cdot G(2)=Ap^{\alpha}=(3^{n}-1)/2=(11\cdots 1)_{ST}$の重みは

$$w = n = p^{\alpha}-p^{\alpha-1} \tag{5.50}$$

である．以上の式(5.48)～(5.50)において，$p\equiv 1(\mathrm{mod}\ 3)$の場合，すべてのけたが1の符号語（式(5.50)）を除いて，符号語の重みはすべて等しく，式(5.48),(5.49)のそれぞれ第1式が最小距離を与える．また，$p\equiv -1(\mathrm{mod}\ 3)$の場合，式(5.48)第2式が最小距離を与える．　（証明終）

法p^{α}に関して3でなく-3が原始根である場合，補題５．４により，法$p^{\alpha-i}$に関して3が属するべき数は，$E(3,p^{\alpha-i})=\varphi(p^{\alpha-i})$／2で奇数である．したがって，補題５．５により，法$2p^{\alpha\ i}$に関して-3は原始根であるが，3は原始根でない．このため，補題３．３により，法$2p^{\alpha-i}$に関して3が属するべき数は，

$$E(3,2p^{\alpha-i}) = \varphi(2p^{\alpha-i})/2 = (p^{\alpha-i}-p^{\alpha-i-1})/2, \quad (i=0,1,\cdots,\alpha-1) \qquad (5.51)$$

であり，これらはすべて奇数である．以上により，

$$n = (p^{\alpha}-p^{\alpha-1})/2,\ A = (3^{n}-1)/(2p^{\alpha}) \qquad (5.52)$$

である．

［定理５．10］　法pに関して3でなく-3が原始根なら，$B=2p^{\alpha}$で規定される符号I_Aの最小距離は，

$$d_m = (p^{\alpha}-2p^{\alpha-1})/3 \qquad (5.53)$$

（証明）　補題５．５，５．３により，3でなく-3が法$2p^{\alpha-i}$,法$p^{\alpha-i}$,(i=0,1,$\cdots,\alpha-1$)の原始根である．さらに，補題５．４および式(5.51)により，

$$E(3,2p^{\alpha-i})=E(3,p^{\alpha-i})=(p^{\alpha-i}-p^{\alpha-i-1})/2$$

であり，奇数である．以上により，

$$G(2p^{\alpha-i}) = H_{(1)}(2p^{\alpha-i}) + H_{(2)}(2p^{\alpha-i}),$$

$$H_{(1)}(2p^{\alpha-i}) = \{3^{k} \bmod 2p^{\alpha-i} \mid k=1,2,\cdots,p^{\alpha-i-1}(p-1)/2\},$$

$$H_{(2)}(2p^{\alpha-i}) = -1\cdot H_{(1)}(2p^{\alpha-i}),$$

また，

$$G(p^{\alpha\ i}) = H_{(1)}(p^{\alpha\ i}) + H_{(2)}(p^{\alpha-i}),$$

$$H_{(1)}(p^{\alpha-i}) = \{3^{k} \bmod p^{\alpha-i} \mid k=1,2,\cdots,p^{\alpha-i-1}(p-1)/2\},$$

$$H_{(2)}(p^{\alpha-i}) = -1 \cdot H_{(1)}(p^{\alpha-i})$$

である．それゆえ，$G(p^{\alpha-i})$, $G(2p^{\alpha-i})$共に，各々，２個のコセットに展開され，3の倍数でない元の個数は等しく配分される．　はじめに，部分符号$Ap^{i} \cdot G(2p^{\alpha-i})$について考える．この部分符号に含まれる両素符号の重みは定理５．９の証明で得られた式(5.47)を利用できる．このとき，補題５．３により，-3が法pに関する原始根であるから，$p \equiv -1 \pmod 3$の場合のみを考えればよい．したがって，式(5.48)により，これらの素符号の重みの最小値は

$$w(\alpha-1) = (p^{\alpha} - 2p^{\alpha-1})/3 \qquad (5.54)$$

である．次に，$A2p^{i} \cdot G(p^{\alpha-i})$については，定理５．８で示した部分符号$Ap^{i} \cdot G(p^{\alpha-i})$に等しい．$p \equiv -1 \pmod 3$の場合，$i=\alpha-2$のときに素符号$A2p^{\alpha-2} \cdot H_{(1)}(p^{2})$の重みが最小となり，

$$w(\alpha-2) = (p^{\alpha} - p^{\alpha-1} - 2p^{\alpha-2})/3 \qquad (5.55)$$

最後に，素符号$Ap^{\alpha} \cdot G(2) = (11\cdots1)_{ST}$の重みは，

$$w = n = (p^{\alpha} - p^{\alpha-1})/2 \qquad (5.56)$$

である．以上の式(5.54)～(5.60)において，式(5.54)がこの符号の最小距離を与える．　（証明終）

(f)　$B=4p^{\alpha}$

法$B=4p^{\alpha}$に関する既約剰余系$G(4p^{\alpha})$の位数は，

$$\varphi(4p^{\alpha}) = p^{\alpha} - p^{\alpha-1} \qquad (5.57)$$

である．$B=2p^{\alpha}$の約数が $1, p, p^{2}, \cdots, p^{\alpha}, 2, 2p, 2p^{2}, \cdots, 2p^{\alpha}$であるから，このような符号語数Bで規定される符号 I_{Δ} は，

$$I_{\Delta} = A \cdot G(4p^{\alpha}) + Ap \cdot G(4p^{\alpha-1}) + \cdots + Ap^{\alpha} \cdot G(4)$$
$$+ A2 \cdot G(2p^{\alpha}) + A2p \cdot G(2p^{\alpha-1}) + \cdots + A2p^{\alpha} \cdot G(2)$$

$$+ A4\cdot G(p^{\alpha}) + A4p\cdot G(p^{\alpha-1}) + \cdots + A4p^{\alpha}\cdot G(1),$$
$$(G(1)=\{0\},\ G(2)=\{1\},\ G(4)=\{\pm 1\}) \qquad (5.58)$$

のように，$3(\alpha+1)$個の部分符号に展開される．

[補題５．６]　法p^{α}に関して3が原始根であり，4がp-1を整除するなら，

$$3^{g} \equiv -1 (\mathrm{mod}\ 4p^{\alpha-i}),\ (0<g<p^{\alpha-i}-p^{\alpha-i-1}, i=0,1,\cdots,\alpha-1) \qquad (5.59)$$

である．

（証明）　付録参照

法p^{α}に関して3が原始根であり，4がp-1を整除するとき，$E(3,p^{\alpha})=p^{\alpha}-p^{\alpha-1}$が偶数であり，$E(3,4)=2$であるから，

$$E(3,4p^{\alpha}) = LCM\{E(3,4),E(3,p^{\alpha})\}$$
$$= p^{\alpha}-p^{\alpha-1} = \varphi(4p^{\alpha})/2 \qquad (5.60)$$

であるから．

$$n = p^{\alpha}-p^{\alpha-1},\ A = (3^{n}-1)/(4p^{\alpha}) \qquad (5.61)$$

である．

[定理５．11]　法p^{α}に関して3が原始根であり，4 がp-1を整除するなら，$B=4p^{\alpha}$で規定される符号 I_B の最小距離は

$$d_m = 2(p^{\alpha}-2p^{\alpha-1})/3,\ (p\equiv -1\ (\mathrm{mod}\ 3)) \qquad (5.62)$$

である．

（証明）はじめに，部分符号$Ap^{i}\cdot G(4p^{\alpha-i})$を考える．補題５．３により，3は

法$p^{\alpha-i}$に関しても原始根であるから，法$4p^{\alpha-i}$に関して3が属するべき数は，

$$E(3,4p^{\alpha-i}) = LCM\{E(3,4),E(3,p^{\alpha-i})\}$$
$$= p^{\alpha-i}-p^{\alpha-i-1} = \varphi(4p^{\alpha-i})/2,$$
$$(i=0,1,\cdots,\alpha-1) \qquad (5.63)$$

である．さらに，補題５．７により，

$$G(4p^{\alpha-i}) = H_{(1)}(4p^{\alpha-i}) + H_{(2)}(4p^{\alpha-i}),$$
$$H_{(1)}(4p^{\alpha-i}) = \{3^k \bmod 4p^{\alpha-i} \mid k=1,2,\cdots,p^{\alpha-i-1}(p-1)/2\},$$
$$H_{(2)}(4p^{\alpha-i}) = -1\cdot H_{(1)}(4p^{\alpha-i}),$$

である．このため，部分符号$Ap^i\cdot G(4p^{\alpha-i})$は，2個の素符号に展開され，両素符号の重みは相等しい．素符号$Ap^i\cdot H_{(1)}(4p^{\alpha-i})$の重み$w(i)$は，$n=p^{\alpha}-p^{\alpha-1}$が$E(3,4p^{\alpha-i})=p^{\alpha-i}-p^{\alpha-i-1}$の$p^i$倍であることにより，

$$w(i) = p^i \times \#\{e \mid e\in H_{(1)}(4p^{\alpha-i}),\ (3,e)=1\}$$
$$= p^i/2 \times \#\{e' \mid e'\in G(4p^{\alpha-i}),\ (3,e')=1\}$$

で与えられる．$G(4p^{\alpha-i})$は，集合

$$S_1 = \{\pm q \mid q=1,2,\cdots,2p^{\alpha-i}\}$$

から，2の倍数の集合

$$S_2 = \{\pm 2j \mid j=1,2,\cdots,p^{\alpha-i}\}$$

とpの倍数の集合

$$S_3 = \{\pm pj \mid j=1,2,\cdots,2p^{\alpha-i-1}\}$$

を除き，2pの倍数の集合

$$S_4 = \{\pm 2pj \mid j=1,2,\cdots,p^{\alpha-i-1}\}$$

を加えて補正したものである．さらに，これら（S_1～S_4）の元のうち各々から3の倍数を除くことにより，

$$w(i) = \begin{cases} 2(p^{\alpha} - p^{\alpha-1} + p^{i})/3, & (\alpha - i \equiv 0 (\mathrm{mod}\ 2)), \\ 2(p^{\alpha} - p^{\alpha-1} - p^{i})/3, & (\alpha - i \equiv 1 (\mathrm{mod}\ 2)) \end{cases} \qquad (5.64)$$

である．ここに，補題５．３，５．１により，法pに関して-3が原始根であるから，$p \not\equiv 1 \pmod 3$である．$p \equiv -1$の場合，最小の重みを持つ素符号は，$i = \alpha - 1$であるから．式(5.63)の第3式により，

$$w(\alpha-1) = 2(p^{\alpha} - 2p^{\alpha-1})/3 \qquad (5.65)$$

を得る．次に，部分符号$A2p^{i} \cdot G(2p^{\alpha-i})$については，定理５．９の部分符号$Ap^{i} \cdot G(2p^{\alpha-i})$に等しく，式(5.48)の第2式から，

$$w(\alpha-1) = 2(p^{\alpha} - 2p^{\alpha-1})/3 \qquad (5.66)$$

である．さらに，部分符号$A4p^{i} \cdot G(p^{\alpha-i})$については，定理５．９の部分符号$A2p^{i} \cdot G(p^{\alpha-i})$に等しく，式(5.49)の第2式から，

$$w(\alpha-2) = 2(p^{\alpha} - p^{\alpha-1} - 2p^{\alpha-2})/3 \qquad (5.67)$$

である．残りの素符号については，

$$Ap^{\alpha} \cdot G(4) = \pm Ap^{\alpha} = (1\bar{1}1\bar{1}\cdots 1\bar{1})_{ST} \text{ または } (\bar{1}1\bar{1}1\cdots\bar{1}1)_{ST}$$

$$A2p^{\alpha} \cdot G(2) = A2p^{\alpha} = (11\cdots 1)_{ST}$$

であるから，これらの素符号の重みは

$$w = n = p^{\alpha} - p^{\alpha-1} \qquad (5.68)$$

である．以上，式(5.64)～(5.67)により，このような符号の最小距離は式(5.64)(5.65)により与えられる．　（証明終）

法p^{α}に関して3でなく-3が原始根であるとき，補題５．４により，法$p^{\alpha-i}$に関して3が属するべき数が，

$$E(3, p^{\alpha-i}) = (p^{\alpha-i} - p^{\alpha-i-1})/2, \quad (i = 0, 1, \cdots, \alpha-1) \qquad (5.69)$$

であり，これは奇数であるから，法$4p^{\alpha-i}$に関して3が属するべき数は

$$E(3,4p^{\alpha-i}) = LCM\{E(3,4),E(3,p^{\alpha-i})\}$$
$$= p^{\alpha-i}-p^{\alpha-i-1} = \varphi(4p^{\alpha-i})/2,$$
$$(i=0,1,\cdots,\alpha-1) \qquad (5.70)$$

である．したがって，

$$n = E(3,4p^{\alpha}) = p^{\alpha}-p^{\alpha-1},\quad A = (3^n-1)/(4p^{\alpha}) \qquad (5.71)$$

[補題５．７]　法p^{α}に関して3でなく-3が原始根なら，

$$3^g \equiv -1 \pmod{4p^{\alpha-i}},\ (0<g<p^{\alpha-i}-p^{\alpha-i-1},\ i=0,1,\cdots,\alpha-1) \qquad (5.72)$$

である．

（証明）　付録参照

[定理５．12]　法pに関して3でなく-3が原始根なら，$B=4p^{\alpha}$で規定される符号I_aの最小距離は，

$$d_m = 2(p^{\alpha}-2p^{\alpha-1})/3 \qquad (5.73)$$

である．

（証明）　はじめに，部分符号 $Ap^i \cdot G(4p^{\alpha-i})$ を考える．式(5.70)の $E(3,4p^{\alpha-i})$と上の補題５．７により，

$$G(4p^{\alpha-i}) = H_{(1)}(4p^{\alpha-i}) + H_{(2)}(4p^{\alpha-i}),$$
$$H_{(1)}(4p^{\alpha\ i}) = \{3^k \bmod 4p^{\alpha-i} \mid k=1,2,\cdots,p^{\alpha\ i-1}(p-1)/2\},$$
$$H_{(2)}(4p^{\alpha-i}) = -1 \cdot H_{(1)}(4p^{\alpha-i}),$$

のように展開される．$G(4p^{\alpha-i})$の元のうち，3の倍数でないものが2個のコセットに等しく配分される．補題５．３により，-3が法pに関する原始根であるから，$p\equiv -1 \pmod 3$ の場合のみを考える．定理５．11の証明で得られる式(5.65)から，これらの部分符号に含まれる素符号の重みの最小値は，

$$w(i) = (p^{\alpha} - 2p^{\alpha-1})/3 \qquad (5.74)$$

である．次に，$A2p^{i}\cdot G(2p^{\alpha-i})$，$A4p^{i}\cdot G(p^{\alpha-i})$,$(i=0,1,2,\cdots,\alpha-1)$については，定理５．10で述べた部分符号$Ap^{i}\cdot G(2p^{\alpha\ i})$，$A2p^{i}\cdot G(p^{\alpha-i})$に等しく，これらに含まれる素符号の重みの最小値は，それぞれ，

$$w(\alpha-1) = (p^{\alpha} - 2p^{\alpha-1})/3 \qquad (5.75)$$

$$w(\alpha-2) = (p^{\alpha} - p^{\alpha-1} - 2p^{\alpha-2})/3 \qquad (5.76)$$

で与えられる．残りの素符号については，定理５．11の場合と同様であり，それらの重みは

$$w = n = p^{\alpha} - p^{\alpha-1} \qquad (5.77)$$

である．以上の式(5.74)～(5.77)において，式(5.74),(5.75)が最小距離を与える．

（証明終）

５．５　符号語数$B=2^{\gamma}$で規定される符号

(g)　$B=2^{\gamma}$

基数3は法2,2^2に関する原始根であるが，γが3以上の場合，3,-3はいずれも法2^{γ}に関する原始根でない．符号語数B=2の場合，符号長はn=1，生成数はA=1であり，符号語は0と1である．その最小距離は1であってＡＮ符号として有効でない．B=4の場合，n=2，A=2であり，その符号語は -2,0,2,4 の4個であって，最小距離は2である．したがって，１誤り検出が可能であるが，符号語数が4では実用性が

ない．１誤り検出符号としては，むしろ，A=2の一般のＳＴ－ＡＮ符号（３．４．1参照）がよい．以下では，γが3以上の場合を考える．

法2^{γ}に関する既約剰余系$G(2^{\gamma})$は，$2^{\gamma-1}$個の奇数のみからなり，その位数は，

$$\varphi(2^{\gamma}) = 2^{\gamma-1} \tag{5.78}$$

である．

［補題５．８］　γは3以上の整数とする．法2^{γ}に関して3が属するべき数は，

$$E(3,2^{\gamma}) = \varphi(2^{\gamma})/2 = 2^{\gamma-2},\ (\gamma \geqq 3) \tag{5.79}$$

であり，$3^{E(3,2^{\gamma})}-1$を2^{γ}で割った商は奇数である．

（証明）　補題３．９参照

［補題５．９］　γが3以上の整数のとき，

$$3^{g} \equiv -1 \pmod{2^{\gamma}},\ (0<g<2^{\gamma-2}) \tag{5.80}$$

である．

（証明）　補題３．９参照

上の補題５．８，５．９により，既約剰余系$G(2^{\gamma})$は，その部分群$H_{(1)}(2^{\gamma})$により，

$$G(2^{\gamma}) = H_{(1)}(2^{\gamma}) + H_{(2)}(2^{\gamma}),$$

$$H_{(1)}(2^{\gamma}) = \{3^{k} \bmod 2^{\gamma} \mid k=1,2,\cdots,2^{\gamma-2}\},$$

$$H_{(2)}(2^{\gamma}) = (-1)\cdot H_{(1)}(2^{\gamma}) \tag{5.81}$$

のようにコセット展開される．

2^{γ}の約数が $1,2,2^{2},\cdots,2^{\gamma}$ であるから，

$$I_A = A\cdot G(2^{\gamma}) + A2\cdot G(2^{\gamma-1}) + \cdots$$

$$\cdots + A2^{\gamma-2}\cdot G(4) + A2^{\gamma-1}\cdot G(2) + A2^{\gamma}\cdot G(1),$$

$$(G(4)=\{\pm 1\}, G(2)=\{1\}, G(1)=\{0\}) \qquad (5.82)$$

のように，(γ+1)個の部分符号に分解される．

B=2^{γ}で規定される符号 I_A の符号長と生成数は，

$$n = E(3,2^{\gamma}) = 2^{\gamma-2},\ A = (3^n-1)/2^{\gamma} \qquad (5.83)$$

である．

[定理５.13]　符号語数B=2^{γ}($\gamma \geqq 3$)で規定される符号 I_A の最小距離は，

$$d_m = 2^{\gamma-3} \qquad (5.84)$$

である．

（証明）　部分符号$A2^i\cdot G(2^{\gamma-i})$,(i=0,1,$\cdots$,$\gamma$-3) を考える．これは，式(5.81)でも示したように，2個の素符号$A2^i\cdot H_{(1)}G(2^{\gamma-i})$と$-A2^i\cdot H_{(1)}G(2^{\gamma-i})$に展開され，両者の重みは等しい．$n=2^{\gamma-2}$が$H_{(1)}(2^{\gamma-i})$の位数$2^{\gamma-i-2}$の$2^i$倍であるから，この素符号の重みw(i)は，

$$w(i) = 2^i \times \#\{e \mid e\in H_{(1)}(2^{\gamma-i}),\ (3,e)=1\}$$

で与えられる．$G(2^{\gamma-i})$は，集合

$$S_1 = \{\pm q \mid q=1,2,\cdots,2^{\gamma-i-1}\}$$

から，2の倍数の集合

$$S_2 = \{\pm 2j \mid j=1,2,\cdots,2^{\gamma-i-2}\}$$

を除いたものである．さらに，この集合から3の倍数を除いて残った元の個数の$2^i/2=2^{i-1}$倍することにより，

$$w(i) = \begin{cases} 2^{\gamma-1}/3, & (\gamma-i\equiv 0 \pmod 2) \\ (2^{\gamma-1}-2^i)/3, & (\gamma-i\equiv 1 \pmod 2) \end{cases} \qquad (5.85)$$

である．i=γ-3のとき，上式がこの符号の最小距離を与える．　　（証明終）

５．６　符号語数Ｂ＝ｐｑ，２ｐｑで規定される符号

(h)　B=pq

p,qは5以上の相異なる素数である．法B=pqに関する既約剰余系G(pq)の位数は，

$$\varphi(pq) = (p-1)(q-1) \qquad (5.86)$$

である．以下，3が法p,qの両者に関する原始根である場合と法pに関して3が原始根であり，法qに関して3でなく-3が原始根である場合を考えるが，どちらの場合も法pqに関する原始根は存在しない．

pqの約数が1,p,q,pqであるから，B=pqで規定される符号 I_A は，

$$I_A = A\cdot G(pq) + AP\cdot G(q) + Aq\cdot G(p) + Apq\cdot G(1),$$

$$(G(1)=\{0\}) \qquad (5.87)$$

のように，4個の部分符号に分解される．

法pおよび法qの両者に関して3が原始根であり，(p-1,q-1)＝2のとき，法B=pqに関して3が属するべき数は，

$$E(3,pq)=LCM[E(3,p),E(3,q)]=(p-1)(q-1)/2$$

であるから，

$$n = (p-1)(q-1)/2,\ A=(3^n-1)/(pq) \qquad (5.88)$$

である．

[補題５.10]　法p,qに関して3が原始根であり，(p-1,q-1)＝2で，しかも，4がp-1またはq-1を整除するなら，

$$3^g \equiv -1 \pmod{pq},\ 3^g \equiv -1 \pmod{2pq},$$

$$(0<g<(p-1)(q-1)/2) \qquad (5.89)$$

である．

（証明）　付録参照

上の補題と式(5.86),(5.88)により，G(pq)は２個のコセット$H_{(1)}(pq)$,$H_{(2)}(pq)$に展開され，G(pq)の元-1は$H_{(1)}(pq)$でなく$H_{(2)}(pq)$に含まれる．また，補題の条件(p-1,q-1)=2であるから，4｜(p-1) または 4｜(q-1) のどちらか一方が成立する．補題５．２により，-3は法pまたは法qのどちらか一方に関する原始根である．このため，$p\equiv q\equiv 1 \pmod 3$ではあり得ないし，また，$p\equiv q\equiv -1 \pmod 3$でもない．ここでは，4｜(p-1) とする．このようにしても一般性を失わない．このとき，-3は法pに関する原始根であり，法qに関する原始根ではない．このようなp,qに対して，$p\equiv -q\equiv -1 \pmod 3$である．

［定理５．14］　法pおよび法qの両者に関して3が原始根であって，(p-1,q-1)＝2，しかも，4｜(p-1)を整除するなら．B=pqで規定される符号 I_Q の最小距離は，

$$d_m = (p-1)(q-1)/3 \tag{5.90}$$

である．

（証明）　補題５．10により，G(pq)は，

$$G(pq)=H_{(1)}(pq)+H_{(2)}(pq),$$
$$H_{(1)}(pq)=\{3k \bmod pq \mid k=1,2,\cdots,(p-1)(q-1)/2\},$$
$$H_{(2)}(pq)=-1\cdot H_{(1)}(pq) \tag{5.91}$$

である．このため，部分符号$A\cdot G(pq)$は2個の素符号$A\cdot H_{(1)}(pq)$と$A\cdot H_{(2)}(pq)$に分解され，両者の重みは等しい．この素符号の重みwは

$$w=\#\{e \mid e\in H_{(1)}(pq),\ (3,e)=1\}$$
$$=(1/2)\times \#\{e' \mid e'\in G(pq),\ (3,e')=1\} \tag{5.92}$$

で与えられる．G(pq)は，集合

$$S_1=\{\pm j \mid j=1,2,\cdots,(pq-1)/2\}$$

から，pの倍数の集合

$$S_2=\{\pm pj \mid j=1,2,\cdots,(q-1)/2\}$$

とqの倍数の集合

$$S_3=\{\pm qj \mid j=1,2,\cdots,(p-1)/2\}$$

を除いたものである．これら(S_1～S_3)の元のうち，それぞれから3の倍数を除き，

残された元の個数をそれぞれw_1,w_2,w_3とすると，

$$w=(w_1-w_2-w_3)/2$$

である．ここに，定理の条件から，補題５．１，５．２を適用でき，$p\equiv -1$，$q\equiv 1 \pmod 3$の場合のみを考えればよい．

$$w_1=2(pq+1)/3,\ (pq\equiv -1 \pmod 3)$$

$$w_2=2(q-1)/3,\ (q\equiv 1 \pmod 3)$$

$$w_3=2(p+1)/3,\ (p\equiv -1 \pmod 3)$$

であり，

$$w = (p-1)(q-1)/3 \qquad (5.93)$$

を得る．

法p,qに関して3が原始根であるから，$A_p\cdot G(q)$，$A_q\cdot G(p)$はともに強巡回的な素符号である．$E(3,q)=q-1$であるから，素符号$A_p\cdot G(q)$の重みwは，$q\equiv 1 \pmod 3$により，

$$w = \frac{n}{E(3,q)} \times \#\{e \mid G(q),(3,e)=1\}$$

$$= \frac{p-1}{2} \times 2(p+1)/3 = (p-1)(q-1)/3 \qquad (5.94)$$

である．$A_q\cdot G(p)$の場合も，同様にして，$p\equiv -1 \pmod 3$により，

$$w = (p+1)(q-1)/3 \qquad (5.95)$$

である．

以上，式(5.93),(5.94),(5.95)により，この符号の最小距離は式(5.90)で与えられる．　（証明終）

法pに関して3が原始根であり，法qに関して3でなく-3が原始根である場合を考える．ただし，$(p-1,q-1)=2$とする．このとき，$E(3,p)=p-1$であり，$E(3,q)=(q-1)/2$で奇数ある．このため，$(p-1,(q-1)/2)=1$である．以上により，

$$n = (p-1)(q-1)/2,\ A = (3^n-1)/(pq) \qquad (5.96)$$

である．

［補題５.11］　法pに関して3が原始根であり，法qに関して3でなく-3が原始根

なら，

$$3^g \not\equiv -1 \pmod{pq},\ 3^g \not\equiv -1 \pmod{2pq},$$
$$(0<g<(p-1)(q-1)/2) \qquad (5.97)$$

である．

（証明）　付録参照

上の補題により，G(pq)の元-1は，$H_{(1)}(pq)$でなく，$H_{(2)}(pq)$に含まれる．

［定理５.15］　法pに関して3が原始根であり，法qに関して3でなく-3が原始根であって，(p-1,q-1)=2なら，B=pqで規定される符号 I_A の最小距離は，

$$d_m = \begin{cases} [(p-1)(q-1)-4]/3, & (p\equiv q\equiv -1 \pmod 3), \\ (p-1)(q-1)/3, & (p\equiv 1, q\equiv -1 \pmod 3) \end{cases} \qquad (5.98)$$

である．

（証明）　補題５.10により，G(pq)については，定理５.14と同様，式(5.91)が成立し，部分符号A･G(pq)は，2個の素符号に分解され，両者の重みは等しく，この素符号の重みwは式(5.92)で与えられる．定理の条件から，補題５.１を適用でき，$q\equiv -1 \pmod 3$である．定理５.14のw_1, w_2, w_3と，さらにw_1, w_3の$p\equiv -1 \pmod 3$の場合を考慮して，

$$w_1 = \begin{cases} 2(pq-1)/3, & (p\equiv -1 \pmod 3) \\ 2(pq+1)/3, & (p\equiv 1 \pmod 3) \end{cases}$$
$$w_2 = 2(q+1)/3,$$
$$w_3 = \begin{cases} 2(p+1)/3, & (p\equiv -1 \pmod 3) \\ 2(p-1)/3, & (p\equiv 1 \pmod 3) \end{cases}$$

であるから，

$$w = (w_1 - w_2 - w_3)/2$$
$$= \begin{cases} [(p-1)(q-1)-4]/3, & (p\equiv -1 \pmod 3) \\ (p-1)(q-1)/3, & (p\equiv 1 \pmod 3) \end{cases} \qquad (5.99)$$

を得る．

法qに関して3でなく-3が原始根であるから，Ap･G(q)は，2個の素符号に分解され，両者の重みは相等しい．また，E(3,q)=(q-1)/2である．この素符号の重みwは，q ≡-1(mod 3)により，

$$w = \frac{n}{E(3,q)} \times (1/2) \times \#\{e \mid G(q), (3,e)=1\}$$

$$= (p-1) \times \frac{q+1}{3} = \frac{(p-1)(q+1)}{3} \qquad (5.100)$$

である．

法pに関して3が原始根であるから，E(3,p)=p-1であり，Aq･G(p)は，強巡回的な素符号であり，この重みwは，

$$w = \frac{n}{E(3,p)} \times \#\{e \mid G(p), (3,e)=1\}$$

$$= \begin{cases} (p+1)(q-1)/3, & (p \equiv -1(\mathrm{mod}\ 3)) \\ (p-1)(q-1)/3, & (p \equiv 1(\mathrm{mod}\ 3)) \end{cases} \qquad (5.101)$$

である．

以上，式(5.99),(5.100),(5.101)により，式(5.98)を得る．　　（証明終）

(i) B=2pq

法B=2pqに関する既約剰余系G(2pq)の位数は，

$$\varphi(2pq) = (p-1)(q-1) \qquad (5.102)$$

であり，2pqの約数が1,p,q,pq,2,2p,2q,2pqであるから，B=2pqで規定される符号 I_A は，

$$I_A = A\cdot G(2pq) + Ap\cdot G(2q) + Aq\cdot G(2p) + Apq\cdot G(2)$$
$$+ A\cdot G(pq) + AP\cdot G(q) + Aq\cdot G(p) + Apq\cdot G(1) \qquad (5.103)$$

のように，8個の部分符号に分解される．

法p,qに関して3が原始根であり，(p-1,q-1)=2であって，4 | (p-1)の場合を考える．この場合，法B=2pqに関して3が属するべき数は，

$$E(3,2pq) = \mathrm{LCM}[E(3,2),E(3,p),E(3,q)]$$
$$= (p-1)(q-1)/2 = \varphi(2pq)/2$$

であるから，

$$n = (p-1)(q-1)/2,\ A = (3^n-1)/(2pq) \qquad (5.104)$$

である．

［定理５．16］　法pおよび法qの両者に関して3が原始根であって，(p-1,q-1)=2，しかも，4がp-1を整除するなら，B=pqで規定される符号 l_A の最小距離は，

$$d_m = (p-2)(q-1)/3 \qquad (5.105)$$

である．

（証明）　補題５．10により，G(2pq)の元-1は$H_{(1)}(2pq)$でなく$H_{(2)}(2pq)$に含まれ，部分符号A･G(2pq)は2個の素符号A･$H_{(1)}(2pq)$とA･$H_{(2)}(2pq)$に展開され，両者の重みは等しい．この素符号の重みwは，

$$w = 1/2 \times \#\{e \mid e \in G(2pq),\ (3,e)=1\} \qquad (5.106)$$

で与えられる．G(2pq)は，集合

$$S_1 = \{\pm j \mid j=1,2,\cdots,pq-1\}$$

から，2,p,qのそれぞれの倍数の集合

$$S_2 = \{\pm 2j \mid j=1,2,\cdots,(pq-1)/2\},$$

$$S_3 = \{\pm pj \mid j=1,2,\cdots,q-1\}$$

$$S_4 = \{\pm qj \mid j=1,2,\cdots,p-1\}$$

を除き，2p,2qの倍数の集合

$$S_5 = \{\pm 2pj \mid j=1,2,\cdots,(q-1)/2\}$$

$$S_6 = \{\pm 2qj \mid j=1,2,\cdots,(p-1)/2\}$$

を加えて補正したものである．これら(S_1～S_6)の元のうち，それぞれから3の倍数を除き，残された元の個数をそれぞれw_1～w_6とすると，

$$w=(w_1-w_2-w_3-w_4+w_5+w_6)/2$$

である．ここに，定理の条件から，補題５．１，５．２を適用でき，$p \equiv -1$，$q \equiv 1 \pmod 3$の場合のみを考えればよい．

$$w_1=2(2pq-1)/3,\ w_2=2(pq+1)/3,\ w_3=4(q-1)/3,$$

$$w_4=2(2p-1)/3,\ w_5=2(q-1)/3,\ w_6=2(p+1)/3$$

により，

$$w = (p-1)(q-1)/3 \qquad (5.107)$$

を得る．また，部分符号A2･G(pq)は定理５.14の場合と同様であり，式(5.93)により，

$$w = (p-1)(q-1)/3 \qquad (5.108)$$

である．

次に，部分符号Aq･G(2p)を考える．法pに関して3(-3)が原始根であるから，3(-3)は法2pに関しても原始根であり，E(3,2p)＝p-1である．この部分符号は強巡回的な素符号である．この素符号の重みは，定理５.４の第2式により，

$$w = \frac{n}{E(3,2p)} \times \#\{e \mid G(2p), (3,e)=1\}$$

$$= \frac{q-1}{2} \times 2(p-2)/3 = (p-2)(q-1)/3 \qquad (5.109)$$

である．部分符号Ap･G(2q)も同様，その重みは，定理５.４の第1式により，

$$w = \frac{p-1}{2} \times 2(q-1)/3 = (p-1)(q-1)/3 \qquad (5.110)$$

で与えられる．

次に，部分符号A2q･G(p)については，定理５.１の第2式から，

$$w = \frac{n}{E(3,p)} \times \#\{e \mid G(p), (3,e)=1\}$$

$$= \frac{q-1}{2} \times 2(p+1)/3 = (p+1)(q-1)/3 \qquad (5.111)$$

である．部分符号A2p･G(q)についても，定理５.１の第1式から，

$$w = (p-1)(q-1)/3 \qquad (5.112)$$

である．

最後に，Apq･G(2)={Apq}については，

$Apq=(3^n-1)/2=(11\cdots1)_{ST}$

であるから，

$$w = n = (p-1)(q-1)/2 \qquad (5.113)$$

である．

以上，式(5.107)～(5.113)により，素符号Aq･G(2p)の重み（式(5.109)）が最小であり，式(5.105)を得る．　（証明終）

法pに関して3が原始根であり，法qに関して3でなく-3が原始根であって，しかも，(p-1,q-1)=2 の場合を考える．このとき，E(3,q)=(q-1)/2で奇数である．また，法B=2pqに関して3が属するべき数は，

$$E(3,2pq)=(p-1)(q-1)/2=\varphi(2pq)/2$$

であるから，

$$n=(p-1)(q-1)/2,\ A=(3^n-1)/(2pq) \tag{5.114}$$

である．

[定理５.17] 法pに関して3が原始根であり，法qに関して3でなく-3が原始根であって，(p-1)(q-1)=2なら，B=2pqで規定される符号 I_A の最小距離は，

$$d_m=\begin{cases}(p-2)(q-1)/3, & (p\equiv -1(\mathrm{mod}\ 3),p<q),\\ (p-1)(q-2)/3, & (p\equiv 1(\mathrm{mod}\ 3)\ \mathrm{or}\ p\equiv -1(\mathrm{mod}\ 3),p>q))\end{cases} \tag{5.115}$$

である．

（証明） はじめに，部分符号A･G(2pq)を考える．補題５.11により，この部分符号は2個の素符号に分解され，両者の重みは等しく，定理５.16の場合と同様である．式(5.103)に基づいて，定理の条件から，補題５.１を適用でき，q≡-1(mod 3)である．定理５.16のw1～w6に加えて，p≡-1(mod 3)の場合も考慮する．

$$w_1=\begin{cases}4(pq-1)/3, & (p\equiv -1(\mathrm{mod}\ 3))\\ 2(2pq-1)/3, & (p\equiv 1(\mathrm{mod}\ 3)),\end{cases}$$

$$w_2=\begin{cases}2(pq-1)/3, & (p\equiv -1(\mathrm{mod}\ 3))\\ 2(pq+1)/3, & (p\equiv 1(\mathrm{mod}\ 3)),\end{cases}$$

$$w_3=2(2q-1)/3,$$

$$w_4=\begin{cases}2(2p-1)/3, & (p\equiv -1(\mathrm{mod}\ 3))\\ 4(p-1)/3, & (p\equiv 1(\mathrm{mod}\ 3)),\end{cases}$$

$$w_5=2(q+1)/3$$

$$w_6=\begin{cases}2(p+1)/3, & (p\equiv -1(\mathrm{mod}\ 3))\\ 2(p-1)/3, & (p\equiv 1(\mathrm{mod}\ 3))\end{cases}$$

により，

$$w = \begin{cases} [(p-1)(q-1)+2]/3, & (p \equiv -1 (\mathrm{mod}\ 3)) \\ (p-1)(q-1)/3, & (p \equiv 1 (\mathrm{mod}\ 3)) \end{cases} \qquad (5.116)$$

を得る．

部分符号A2･G(pq)は，定理５.15の場合と同様であり，2個の素符号の重みは等しく，

$$w = \begin{cases} [(p-1)(q-1)4]/3, & (p \equiv -1 (\mathrm{mod}\ 3)) \\ (p-1)(q-1)/3, & (p \equiv 1 (\mathrm{mod}\ 3)) \end{cases} \qquad (5.117)$$

である．

部分符号Ap･G(2q)は，2個の素符号に分解され，両者の重みは等しい．また，E(3,2q)=(q-1)/2であり，この素符号の重みは定理５.４の式(5.17)を利用して，

$$w = (p-1)(q-1)/3 \qquad (5.118)$$

である．部分符号Aq･G(2p)は，強巡回的な素符号であり，E(3,2p)=p-1であり，この素符号の重みは，式(5.10),(5.11)を利用して，

$$w = \frac{q-1}{2} \times \#\{e \mid e \in G(2p), (3,e)=1\}$$

$$= \begin{cases} (p-2)(q-1)/3, & (p \equiv -1 (\mathrm{mod}\ 3)) \\ (p-1)(q-1)/3, & (p \equiv 1 (\mathrm{mod}\ 3)) \end{cases} \qquad (5.119)$$

を得る．

部分符号A2p･G(q)の場合は，定理５.15の証明から，この素符号の重みは式(5.100)で与えられる．

$$w = (p-1)(q+1)/3 \qquad (5.120)$$

である．部分符号Aq･G(p)の場合も，定理５.15の証明から，重みは式(5.101)で与えられ，

$$w = \begin{cases} (p+1)(q-1)/3, & (p \equiv -1 (\mathrm{mod}\ 3)) \\ (p-1)(q-1)/3, & (p \equiv 1 (\mathrm{mod}\ 3)) \end{cases} \qquad (5.121)$$

である．

以上，式(5.116)～(5.121)により，式(5.115)を得る．　　（証明終）

５．７　符号語数$B=p^{\alpha}q, 2p^{\alpha}q$で規定される符号

(j)　$B=p^{\alpha}q$

p,qは相異なる5以上の素数，αは2以上の整数である．法$B=p^{\alpha}q$に関する既約剰余系$G(p^{\alpha}q)$の位数は，

$$\varphi(p^{\alpha}q) = (p^{\alpha}-p^{\alpha-i})(q-1) \qquad (5.122)$$

である．符号語数$B=p^{\alpha}q$で規定される符号 I_A は，

$$I_A = A\cdot G(p^{\alpha}q) + Ap\cdot G(p^{\alpha-1}q) + \cdots + Ap^{\alpha}\cdot G(q)$$
$$+ Aq\cdot G(p^{\alpha}) + Apq\cdot G(p^{\alpha-1}) + \cdots + Ap^{\alpha}q\cdot G(1),$$
$$(G(1)=\{0\}) \qquad (5.123)$$

のように，$2(\alpha+1)$個の部分符号に分解される．以下では，

(1) 法p^{α},qに関して3が原始根である場合，

(2) 法p^{α}に関して3が原始根であり，法qに関して3でなく-3が原始根である場合，

(3) 法p^{α}に関して3でなく-3が原始根であり，法qに関して3が原始根である場合

の３つの場合について検討する．

(1)の場合，(h)のB=pqの場合と同様，$(p^{\alpha}-p^{\alpha-1}, q-1)=2$ で，$4 \mid (p-1)$ または $4 \mid (q-1)$なる条件を付け加える．このとき，

$$n = E(3,p^{\alpha}q) = LCM[E(3,p^{\alpha}),E(3,q)]$$
$$= p^{\alpha-1}(p-1)(q-1)/2,$$
$$A = (3^n-1)/(2p^{\alpha}q) \qquad (5.124)$$

である．

［補題５.12］　法p^{α},qに関して3が原始根であり，$(p^{\alpha}-p^{\alpha-1},q-1)=2$，しか

も，4 | (p-1)または4 | (q-1) なら，

$$3^g \equiv -1 \pmod{p^\alpha q},\quad 3^g \equiv -1 \pmod{2p^\alpha q},$$

$$(0<g<(p^{\alpha-i}-p^{\alpha-i-1})(q-1)/2;\ \ i=0,1,\cdots,\alpha-1) \qquad (5.125)$$

である．

（証明）　補題５.10と同様に証明される．　（証明終）

上の補題と式(5.122),(5.124)により，$G(p^{\alpha-i}q)$は２個のコセットに展開され，元-1は $H_{(1)}(p^{\alpha-i}q)$でなく$H_{(2)}(p^{\alpha-i}q)$に含まれる．また，補題の条件 $(p^\alpha-p^{\alpha-1},q-1)=2$であるから，4 | (p-1) または 4 | (q-1) のどちらか一方が成立する．補題５.２により，-3は法pまたは法qのどちらか一方に関する原始根である．このため，$p\equiv q\equiv 1 \pmod 3$ではあり得ないし，また，$p\equiv q\equiv -1 \pmod 3$でででもない．

[定理５.18]　法p^α,qに関して3が原始根であって，$(p^\alpha-p^{\alpha-1},q-1)=2$，しかも，4 | (p-1) または 4 | (q-1) なら，$B=p^\alpha q$で規定される符号 l_B の最小距離は

$$d_m = \begin{cases} (p^\alpha-p^{\alpha-1})(q-1)/3, & (p\equiv 1, q\equiv -1 \pmod 3) \\ (p^\alpha-p^{\alpha-1}-2p^{\alpha-2})(q-1)/3, & (p\equiv -1, q\equiv 1 \pmod 3) \end{cases} \qquad (5.126)$$

である．

（証明）　はじめに，部分符号$A_p{}^i \cdot G(p^{\alpha-i}q),(i=0,1,\cdots,\alpha-1)$を検討する．

$$\varphi(p^{\alpha-i}q)=(p^{\alpha-i}-p^{\alpha-i-1})(q-1),$$

$$E(3,p^{\alpha-i}q)=(p^{\alpha-i}-p^{\alpha-i-1})(q-1)/2 \qquad (5.127)$$

であるから，$G(p^{\alpha-i}q)$は，2個のコセットに展開され，補題５.12により，この部分符号は，２個の素符号に分解され両者の重みは等しい．符号長 n が $G(p^{\alpha-i}q)$ の位数$\varphi(pq)=(p^{\alpha-i}-p^{\alpha-i-1})(q-1)$の$p^i/2$倍であるから，この素符号

の重みwは，

$$w = p^{i} \times (1/2) \times \#\{e \mid e \in G(p^{\alpha-i}q),\ (3,e)=1\}$$

で与えられる．$G(p^{\alpha-i}q)$は，集合

$$S_1=\{\pm j \mid j=1,2,\cdots,(p^{\alpha-i}q-1)/2\}$$

から，pの倍数の集合とqの倍数の集合

$$S_2=\{\pm pj \mid j=1,2,\cdots,(p^{\alpha-i-1}q-1)/2\},$$

$$S_3=\{\pm qj \mid j=1,2,\cdots,(p^{\alpha-i}-1)/2\}$$

を除き，pqの倍数の集合

$$S_4=\{\pm pqj \mid j=1,2,\cdots,(p^{\alpha-i-1}-1)/2\},$$

を加えて補正したものである．これら(S_1～S_4)の元のうち，それぞれから3の倍数を除き，残された元の個数それぞれw_1～w_4とすると，これらに属する素符号の重み$w(i)$は

$$w(i)=p^{i}(w_1-w_2-w_3+w_4)/2$$

である．このとき，

$$w_1=\begin{cases}2(p^{\alpha-i}q-1)/3, & (p^{\alpha-i}q\equiv 1 \pmod 3)\\ 2(p^{\alpha-i}q+1)/3, & (p^{\alpha-i}q\equiv -1 \pmod 3)\end{cases}$$

$$w_2=\begin{cases}2(p^{\alpha-i-1}q-1)/3, & (p^{\alpha-i-1}q\equiv 1 \pmod 3)\\ 2(p^{\alpha-i-1}q+1)/3, & (p^{\alpha-i-1}q\equiv -1 \pmod 3)\end{cases}$$

$$w_3=\begin{cases}2(p^{\alpha-i}-1)/3, & (p^{\alpha-i}\equiv 1 \pmod 3)\\ 2(p^{\alpha-i}+1)/3, & (p^{\alpha-i}\equiv -1 \pmod 3)\end{cases}$$

$$w_4=\begin{cases}2(p^{\alpha-i-1}-1)/3, & (p^{\alpha-i-1}\equiv 1 \pmod 3)\\ 2(p^{\alpha-i-1}+1)/3, & (p^{\alpha-i-1}\equiv -1 \pmod 3)\end{cases}$$

である．ここに，定理の条件から，$p\equiv -1$, $q\equiv 1 \pmod 3$と$p\equiv 1$, $q\equiv -1 \pmod 3$の場合を考える．いずれの場合も，$w(i)$の最小値wは$i=\alpha-1$であり，

$$w = (p^{\alpha}-p^{\alpha-1})(q-1)/3 \qquad (5.128)$$

を得る．

次に，部分符号$Ap^{\alpha}\cdot G(q)$を考える．法qに関して3が原始根であるから，この部分符号は強巡回的な素符号である．この素符号の重みは，

$$w = \frac{n}{q-1} \times \#\{e \mid e\in G(q),\ (3,e)=1\}$$

で与えられる．$n=(p^{\alpha}-p^{\alpha-1})(q-1)/2$であるから，これらの素符号の重みwは

$$w = \begin{cases} (p^{\alpha}-p^{\alpha-1})(q-1)/3, & (q\equiv 1(\mathrm{mod}\ 3)) \\ (p^{\alpha}-p^{\alpha-1})(q+1)/3, & (q\equiv -1(\mathrm{mod}\ 3)) \end{cases} \qquad (5.129)$$

である．

最後に，部分符号$Ap^{i}q\cdot G(p^{\alpha-i})$を考える．これらの部分符号は，補題５．３により，それぞれ，強巡回的な素符号である．$E(3,p^{\alpha-i})=p^{\alpha-i-1}(p-1)$であるから，

$$w(i)= \frac{n}{p^{\alpha-i-1}(p-1)} \times \#\{e \mid e\in G(p^{\alpha-i}),\ (3,e)=1\}$$

で与えられる．$G(p^{\alpha-i})$は，定理５．７の場合と同様にして，最小値wは

$$w = \begin{cases} (p^{\alpha}-p^{\alpha-1})(q-1)/3, & (p\equiv 1(\mathrm{mod}\ 3)) \\ (p^{\alpha}-p^{\alpha-1}-2p^{\alpha-2})(q-1)/3, & (p\equiv -1(\mathrm{mod}\ 3)) \end{cases} \qquad (5.130)$$

である．

以上，式(5.128)～(5.130)により，(5.126)を得る．　　（証明終）

(2)の場合を考える．このとき，符号長nと生成数Aは，(1)の場合の式(5.124)に一致する．

[補題５.13]　法p^{α}に関して3が原始根であり，法qに関して3でなく-3が原始根であって，$(p^{\alpha}-p^{\alpha-1},q-1)=2$ なら，

$$3^{g} \not\equiv -1\ (\mathrm{mod}\ p^{\alpha-i}q),\ 3^{g} \not\equiv -1\ (\mathrm{mod}\ 2p^{\alpha-i}q),$$
$$(0<g<(p^{\alpha-i}-p^{\alpha-i-1})(q-1)/2,\ (i=0,1,\cdots,\alpha-1)) \qquad (5.131)$$

である．

（証明）　補題５.11と同様にして証明される．　　（証明終）

[定理５.19]　法p^{α} に関して3が原始根であり，法qに関して3でなく-3が原始根であって，$(p^{\alpha}-p^{\alpha-1},q-1)=2$ なら，$B=p^{\alpha}q$で規定される符号 I_A の最小距離は

$$d_m = \begin{cases} (p^{\alpha}-p^{\alpha-1})(q-1)/3, & (p\equiv 1(\mathrm{mod}\ 3)) \\ (p^{\alpha}-p^{\alpha-1}-2p^{\alpha-2})(q-1)/3, & (p\equiv -1(\mathrm{mod}\ 3),\ 2p+1<q) \\ [(p^{\alpha}-p^{\alpha-1})(q-1)-4p^{\alpha-1}]/3, & (p\equiv -1(\mathrm{mod}\ 3),\ 2p+1>q) \end{cases} \tag{5.132}$$

である．

（証明）　はじめに，部分符号$Ap^{i}\cdot G(p^{\alpha-i}q),(i=0,1,\cdots,\alpha-1)$を検討する．

$$\varphi(p^{\alpha-i}q)=(p^{\alpha-i}-p^{\alpha-i-1})(q-1),$$

$$E(3,p^{\alpha-i}q)=(p^{\alpha\ i}-p^{\alpha-i-1})(q-1)/2$$

であるから，補題５.13により，この部分符号は，２個の素符号に分解され両者の重みは等しい．これらの素符号の重みの最小値wを求める手順は定理５.18の対応する部分符号と同様である．ただし，$q\equiv -1(\mathrm{mod}\ 3)$であることを考慮すれば，

$$w = \begin{cases} [(p^{\alpha}-p^{\alpha-1})(q-1)-4p^{\alpha-1}]/3, & (p\equiv -1(\mathrm{mod}\ 3)) \\ (p^{\alpha}-p^{\alpha-1})(q-1)/3, & (p\equiv 1(\mathrm{mod}\ 3)) \end{cases} \tag{5.133}$$

である．

次に，部分符号$Ap^{\alpha}\cdot G(q)$を考える．法qに関して3でなく-3が原始根であるから，E(3,q)=(q-1)/2であり，これが奇数である．このため．この部分符号は2個の素符号からなり，両素符号の重みwは等しく，定理５.２を利用して，

$$w = (p^{\alpha}-p^{\alpha-1})(q+1)/3 \tag{5.134}$$

が得られる．

最後に，部分符号$Ap^{i}_{q}\cdot G(p^{\alpha-i})$を考える．これらの部分符号は(1)の場合と同じであり，式(5.30)で得られる．

以上により，式(5.132)を得る．　（証明終）

(3)の場合を考える．このとき，補題５．４により，

$$E(3,p^{\alpha-i})=(p^{\alpha-i}-p^{\alpha-i-1})/2,\ (i=0,1,\cdots,\alpha-1)$$

であり，これらは奇数である．また，$E(3,q)=q-1$であり，$(p-1,q-1)=2$であるから，

$$E(3,p^{\alpha}q)=(p^{\alpha}-p^{\alpha-1})(q-1)/2 \qquad (5.135)$$

である．このため，このような符号の符号長と生成数は，(1),(2)の場合と同じである．

[補題５．14]　法p^{α}に関して3でなく-3が原始根であり，法qに関して3が原始根であって，$(p^{\alpha}-p^{\alpha-1},q-1)=2$ なら，

$$3^{g}\not\equiv -1\ (\mathrm{mod}\ p^{\alpha-i}q),\ 3^{g}\not\equiv -1\ (\mathrm{mod}\ 2p^{\alpha-i}q),$$

$$(0<g<(p^{\alpha-i}-p^{\alpha-i-1})(q-1)/2,\ (i=0,1,\cdots,\alpha-1)) \qquad (5.136)$$

である．

（証明）　補題５．11と同様にして証明される．　（証明終）

[定理５．20]　法p^{α}に関して3でなく-3が原始根であり，法qに関して3が原始根であって，$(p^{\alpha}-p^{\alpha-1},q-1)=2$ なら，$B=p^{\alpha}q$で規定される符号 l_Aの最小距離は

$$d_m=\begin{cases}(p^{\alpha}-p^{\alpha-1})(q-1)/3, & (p\equiv 1(\mathrm{mod}\ 3))\\ (p^{\alpha}-p^{\alpha-1}-2p^{\alpha-2})(q-1)/3, & (p\equiv -1(\mathrm{mod}\ 3),\ 2p+1<q)\\ [(p^{\alpha}-p^{\alpha-1})(q-1)-4p^{\alpha-1}]/3, & (p\equiv -1(\mathrm{mod}\ 3),\ 2p+1>q)\end{cases} \qquad (5.137)$$

である．

（証明） はじめに，部分符号$Ap^{i}\cdot G(p^{\alpha-i}q),(i=0,1,\cdots,\alpha-1)$を検討する．これらの部分符号は，式(5.122),(5.135)により，2個の素符号に分解され，上の補題により，両者の重みは等しい．これらの素符号の重みの最小値wを求める手順は定理５.18の対応する部分符号と同様である．ただし，$p\equiv -1(\mathrm{mod}\ 3)$であることを考慮すれば，

$$w=\begin{cases}(p^{\alpha}-p^{\alpha-1}-2p^{\alpha-2})(q-1)/3, & (q\equiv 1(\mathrm{mod}\ 3))\text{または}\\ & (q\equiv -1(\mathrm{mod}\ 3),\ 2p+1<q)\\ [(p^{\alpha}-p^{\alpha-1})(q-1)-4p^{\alpha-1}]/3, & (p\equiv -1(\mathrm{mod}\ 3),\ 2p+1>q)\end{cases} \tag{5.138}$$

である．

次に，部分符号$Ap^{\alpha}\cdot G(q)$を考える．法qに関して3が原始根であるから，E(3, q)=(q-1)であり，この部分符号は強巡回的な素符号であり，式(5.129)と同じである．

最後に，部分符号$Ap^{i}q\cdot G(p^{\alpha-i})$を考える．これらの部分符号は，補題５.４により，2個の素符号に展開され，両者に展開され，両者の重みは等しい．また，

$$E(3,p^{\alpha-i})=(p^{\alpha-i}-p^{\alpha-i-1})/2$$

であるから，その重みw(i)は，

$$w(i)=\frac{n}{p^{\alpha-i-1}(p-1)/2}\times(1/2)\times \#\{e\mid e\in G(p^{\alpha-i}),(3,e)=1\}$$

$$=p^{i}(q-1)\times(1/2)\times \#\{e\mid e\in G(p^{\alpha-i}),(3,e)=1\}$$

であり，定理５.８の証明中の式(5.38)の第２,第３式を利用して，それらの最小値wは

$$w=(p^{\alpha}-p^{\alpha-1}-2p^{\alpha-2})(q-1)/3 \tag{5.139}$$

である．

以上，式(5.138),(5.129),(5.139)により，式(5.137)を得る． （証明終）

(k) $B=2p^{\alpha}q$

法$B=2p^{\alpha}q$に関する既約剰余系$G(2p^{\alpha}q)$の位数は，

$$\varphi(2p^{\alpha}q) = (p^{\alpha}-p^{\alpha-1})(q-1) \qquad (5.140)$$

である．符号語数$B=2p^{\alpha}q$で規定される符号 l_A は，

$$\begin{aligned} l_A = {} & A\cdot G(2p^{\alpha}q) + Ap\cdot G(2p^{\alpha-1}q) + \cdots + Ap^{\alpha}\cdot G(2q) \\ & + A2\cdot G(p^{\alpha}q) + A2p\cdot G(p^{\alpha-1}q) + \cdots + A2p^{\alpha}\cdot G(q) \\ & + Aq\cdot G(2p^{\alpha}) + Apq\cdot G(2p^{\alpha-1}) + \cdots + Ap^{\alpha}q\cdot G(2) \\ & + A2q\cdot G(p^{\alpha}) + A2pq\cdot G(p^{\alpha-1}) + \cdots + A2p^{\alpha}q\cdot G(1), \\ & \qquad (G(2)=\{1\}, G(1)=\{0\}) \qquad (5.141) \end{aligned}$$

のように，$4(\alpha+1)$個の部分符号に分解される．以下では，

(1) 法p^{α},qに関して3が原始根である場合，

(2) 法p^{α}に関して3が原始根であり，法qに関して3でなく-3が原始根である場合，

(3) 法p^{α}に関して3でなく-3が原始根であり，法qに関して3が原始根である場合

の３つの場合について検討する．

(1)の場合，(j)と同様に，$(p^{\alpha}-p^{\alpha-1},q-1)=2$，しかも，$4\mid(p-1)$または $4\mid(q-1)$なる条件を付加する．このとき，

$$\begin{aligned} n &= E(3,2p^{\alpha}q) = LCM[E(3,2),E(3,p^{\alpha}),E(3,q)] \\ &= (p^{\alpha}-p^{\alpha-1})(q-1)/2 = \varphi(2p^{\alpha}q)/2, \\ A &= (3n-1)/(2p^{\alpha}q) \qquad (5.142) \end{aligned}$$

である．

[定理５.21]　法p^{α},qに関して3が原始根であり，$(p^{\alpha}-p^{\alpha-1},q-1)=2$，しかも$4\mid(p-1)$または$4\mid(q-1)$ なら，$B=2p^{\alpha}q$ で規定される符号 l_A の最小距離は，

$$d_m = \begin{cases} (p^{\alpha} - p^{\alpha-1})(q-2)/3, & (p \equiv -q \equiv 1 \pmod 3) \\ (p^{\alpha} - 2p^{\alpha-1})(q-1)/3, & (p \equiv -q \equiv -1 \pmod 3) \end{cases} \qquad (5.143)$$

である．

（証明） はじめに，部分符号$Ap \cdot G(2p^{\alpha-i}q)$を考える．定理の条件と補題５．12により，この部分符号は重みの等しい２個の素符号に展開される．$G(2p^{\alpha-i}q)$は，集合

$$S_1 = \{\pm j \mid j=1,2,\cdots,p^{\alpha}{}^{i}q\}$$

から，2,p,qの各々の倍数の集合

$$S_2 = \{\pm 2j \mid j=1,2,\cdots,(p^{\alpha-i}q-1)/2\},$$

$$S_3 = \{\pm pj \mid j=1,2,\cdots,p^{\alpha-i-1}q\}$$

$$S_4 = \{\pm qj \mid j=1,2,\cdots,p^{\alpha-i}\}$$

を除き，2p,pq,2qの倍数の集合

$$S_5 = \{\pm 2pj \mid j=1,2,\cdots,(p^{\alpha-i-1}q-1)/2\}$$

$$S_6 = \{\pm pqj \mid j=1,2,\cdots,p^{\alpha-i-1}-1\}$$

$$S_7 = \{\pm 2qj \mid j=1,2,\cdots,(p^{\alpha-i}-1)/2\}$$

を加え，さらに，2pqの倍数の集合

$$S_8 = \{\pm 2pqj \mid j=1,2,\cdots,(p^{\alpha-i-1}-1)/2\}$$

を除いて補正したものである．集合S_1～S_2の各々から3の倍数を除いて残った元の個数をそれぞれw_1～w_8とすれば，

$$w_1 = \begin{cases} 2(2p^{\alpha-i}q+1)/3, & (p^{\alpha-i}q \equiv 1 \pmod 3), \\ 4(p^{\alpha-i}q+1)/3, & (p^{\alpha-i}q \equiv -1 \pmod 3) \end{cases}$$

$$w_2=\begin{cases}2(p^{\alpha-i}q-1)/3, & (p^{\alpha-i}q\equiv 1(\mathrm{mod}\ 3)),\\ 2(p^{\alpha-i}q+1)/3, & (p^{\alpha-i}q\equiv -1(\mathrm{mod}\ 3))\end{cases}$$

$$w_3=\begin{cases}2(2p^{\alpha-i-1}q+1)/3, & (p^{\alpha-i-1}q\equiv 1(\mathrm{mod}\ 3)),\\ 4(p^{\alpha-i-1}q+1)/3, & (p^{\alpha-i-1}q\equiv -1(\mathrm{mod}\ 3))\end{cases}$$

$$w_4=\begin{cases}2(2p^{\alpha-i}+1)/3, & (p^{\alpha-i}\equiv 1(\mathrm{mod}\ 3)),\\ 4(p^{\alpha-i}+1)/3, & (p^{\alpha-i}\equiv -1(\mathrm{mod}\ 3))\end{cases}$$

$$w_5=\begin{cases}2(2p^{\alpha-i-1}q-1)/3, & (p^{\alpha-i-1}q\equiv 1(\mathrm{mod}\ 3)),\\ 2(2p^{\alpha-i-1}q+1)/3, & (p^{\alpha-i-1}q\equiv -1(\mathrm{mod}\ 3))\end{cases}$$

$$w_6=\begin{cases}2(2p^{\alpha-i-1}+1)/3, & (p^{\alpha-i-1}\equiv 1(\mathrm{mod}\ 3)),\\ 4(p^{\alpha-i-1}+1)/3, & (p^{\alpha-i-1}\equiv -1(\mathrm{mod}\ 3))\end{cases}$$

$$w_7=\begin{cases}2(p^{\alpha\ i}-1)/3, & (p^{\alpha-i}\equiv 1(\mathrm{mod}\ 3)),\\ 2(p^{\alpha-i}+1)/3, & (p^{\alpha-i}\equiv -1(\mathrm{mod}\ 3))\end{cases}$$

$$w_8=\begin{cases}2(p^{\alpha-i-1}-1)/3, & (p^{\alpha-i-1}\equiv 1(\mathrm{mod}\ 3)),\\ 2(p^{\alpha-i-1}+1)/3, & (p^{\alpha-i-1}\equiv -1(\mathrm{mod}\ 3))\end{cases}$$

である．これらに属する素符号の重み$w(i)$は

$$w(i) = p^i \times (1/2) \times \#\{e \mid e\in G(2p^\alpha q),(3,e)=1\}$$

$$= (p^i/2) \times (w_1-w_2-w_3-w_4+w_5+w_6+w_7-w_8)$$

$$= \begin{cases}[(p^\alpha-p^{\alpha\ 1})(q-1)-2p^i]/3, & (p\equiv q\equiv -1(\mathrm{mod}\ 3),\alpha-i\equiv 0(\mathrm{mod}\ 2))\\ [(p^\alpha-p^{\alpha-1})(q-1)+2p^i]/3, & (p\equiv q\equiv -1(\mathrm{mod}\ 3),\alpha-i\equiv 1(\mathrm{mod}\ 2))\\ (p^\alpha-p^{\alpha-1})(q-1)/3, & (\text{その他})\end{cases}$$

により，これらの最小値wは，

$$w = \begin{cases} [(p^{\alpha}-p^{\alpha-1})(q-1)-2p^{\alpha-2}]/3, & (p\equiv q\equiv -1(\mathrm{mod}\ 3)), \\ (p^{\alpha}-p^{\alpha-1})(q-1)/3, & (\text{その他}) \end{cases} \tag{5.144}$$

このとき，前節の(1)の場合と同様の条件であるから，$p\equiv q\equiv -1$はあり得ず，

$$w = (p^{\alpha}-p^{\alpha-1})(q-1)/3 \tag{5.145}$$

である．

部分符号$A2p^{i}\cdot G(p^{\alpha-i}q)$を考える．これは，定理５.18の証明における部分符号$Ap^{i}\cdot G(p^{\alpha-i}q)$と同じであり，これらに含まれる素符号の最小値wは，式(5.128)で与えられ，

$$w = (p^{\alpha}-p^{\alpha-1})(q-1)/3 \tag{5.146}$$

である．

次に，部分符号$Ap^{i}q\cdot(2p^{\alpha-i})$を考える．補題５.５により，法$2p^{\alpha-i}$に関して3が原始根であるから，

$$E(3,2p^{\alpha-i}) = p^{\alpha-i}-p^{\alpha-i-1} = \varphi(2p^{\alpha-i})$$

であり，これらの部分符号は強巡回的な素符号である．また，$G(2p^{\alpha-i})$は定理５.９の結果を利用して，これらに含まれる素符号の重みw(i)は，

$$w(i)= \frac{p^{i}(q-1)}{2} \times \#\{e \mid e\in G(p^{\alpha-i}),\ (3,e)=1\}$$

であり，これらの素符号の重みの最小値wは，

$$w = \begin{cases} (p^{\alpha}-p^{\alpha-1})(q-1)/3, & (p\equiv 1(\mathrm{mod}\ 3)) \\ (p^{\alpha}-2p^{\alpha-1})(q-1)/3, & (p\equiv 1(\mathrm{mod}\ 3)) \end{cases} \tag{5.147}$$

である．

次に，部分符号$A2p^{i}q\cdot G(p^{\alpha\ i})$を考える．補題５.５により，

$$E(3,p^{\alpha-i}) = p^{\alpha\ i}-p^{\alpha\ i-1}$$

であり，これは強巡回的な素符号であり，$G(p^{\alpha})$は定理５.７の結果を利用でき

て，これらの素符号の重みの最小値wは，

$$w = \begin{cases} (p^{\alpha} - p^{\alpha-1})(q-1)/3, & (p \equiv 1 (\mathrm{mod}\ 3)) \\ (p^{\alpha} - p^{\alpha-1} - 2p^{\alpha-2})(q-1)/3, & (p \equiv -1 (\mathrm{mod}\ 3)) \end{cases} \qquad (5.148)$$

である．

部分符号$Ap^{\alpha} \cdot G(2q)$を考える．$n/E(3,2q) = n/(q-1) = (p^{\alpha} - p^{\alpha-1})/2$であるから，定理５．３の結果を利用でき，この素符号の重みwは，

$$w = \begin{cases} (p^{\alpha} - p^{\alpha-1})(q-1)/3, & (q \equiv 1 (\mathrm{mod}\ 3)) \\ (p^{\alpha} - p^{\alpha-1})(q-2)/3, & (q \equiv -1 (\mathrm{mod}\ 3)) \end{cases} \qquad (5.149)$$

である．また，部分符号$A2p^{\alpha} \cdot G(q)$についても同様であり，定理５．１の結果を利用して，この素符号の重みwは

$$w = \begin{cases} (p^{\alpha} - p^{\alpha-1})(q-1)/3, & (q \equiv 1 (\mathrm{mod}\ 3)) \\ (p^{\alpha} - p^{\alpha-1})(q+1)/3, & (q \equiv -1 (\mathrm{mod}\ 3)) \end{cases} \qquad (5.150)$$

を得る．

最後に，$Ap^{\alpha}q \cdot G(2) = (3^n - 1)/2 = (11\cdots1)_{ST}$であり，この符号語の重みwは，

$$w = n = (p^{\alpha} - p^{\alpha-1})(q-1)/2 \qquad (5.151)$$

である．

以上，式(5.144)～(5.151)により，式(5.143)を得る．　　（証明終）

(2)の場合を考える．このとき，符号長nと生成数Aは，(1)の場合の式(5.142)に一致する．

［定理５．22］　法p^{α}に関して3が原始根であり，法qに関して3でなく-3が原始根であって，$(p^{\alpha} - p^{\alpha-1}, q-1) = 2$なら，$B = 2p^{\alpha}q$ で規定される符号 I_B の最小距離は，

$$d_m = \begin{cases} (p^{\alpha}-p^{\alpha-1})(q-2)/3, & (p\equiv 1(\mathrm{mod}\ 3))\text{または}(p\equiv -1(\mathrm{mod}\ 3), p>q) \\ (p^{\alpha}-2p^{\alpha-1})(q-1)/3, & (p\equiv -1(\mathrm{mod}\ 3), p<q) \end{cases} \quad (5.152)$$

である．

（証明）　はじめに，部分符号$A\cdot G(2p^{\alpha-i}q)$について考える．$G(2p^{\alpha-i}q)$については，補題５.13が成立し，この部分符号は，重みの等しい２個の素符号（式(5.142)）に展開されるため，定理５.21の場合に等しい．法qに関して-3が原始根であるから，$q\not\equiv 1(\mathrm{mod}\ 3)$ なることに注意して，これらの素符号の重みの最小値wは，式(5.144)の第１,第２式で与えられる．すなわち，

$$w = \begin{cases} [(p^{\alpha}-p^{\alpha-1})(q-1)-2p^{\alpha-2}]/3, & (p\equiv q\equiv -1(\mathrm{mod}\ 3)), \\ (p^{\alpha}-p^{\alpha-1})(q-1)/3, & (\text{その他}) \end{cases} \quad (5.153)$$

部分符号$A2p^{i}\cdot G(p^{\alpha-i}q)$を考える．これは，定理５.19の証明における部分符号$Ap^{i}\cdot G(p^{\alpha-i}q)$と同じであり，これらに含まれる素符号の重みの最小値wは，式(5.133)で与えられ，

$$w = \begin{cases} (p^{\alpha}-p^{\alpha-1})(q-1)/3, & (p\equiv 1(\mathrm{mod}\ 3)) \\ [(p^{\alpha}-p^{\alpha-1})(q-1)-4p^{\alpha-1}]/3, & (p\equiv -1(\mathrm{mod}\ 3)) \end{cases} \quad (5.154)$$

である．

部分符号$Ap^{\alpha}\cdot G(2q)$を考える．E(3,2q)=(q-1)/2であり，また，定理５.４の結果を利用でき，この素符号の重みwは，

$$w = (p^{\alpha}-p^{\alpha-1})(q-2)/3 \quad (5.155)$$

である．また，部分符号$A2p^{\alpha}\cdot G(q)$についても同様であり，定理５.２の結果を利用して，この素符号の重みwは

$$w = (p^{\alpha}-p^{\alpha-1})(q+1)/3 \quad (5.156)$$

である．

次に，部分符号$Ap^{i}q\cdot(2p^{\alpha-i})$については，(1)の場合と同じものであり，これ

らの素符号の重みの最小値wは，

$$w = \begin{cases} (p^{\alpha} - p^{\alpha-1})(q-1)/3, & (p \equiv 1 (\mathrm{mod}\ 3)) \\ (p^{\alpha} - 2p^{\alpha-1})(q-1)/3, & (p \equiv -1 (\mathrm{mod}\ 3)) \end{cases} \qquad (5.157)$$

である．また，部分符号$A2p^{i}q \cdot G(p^{\alpha-i})$についても同様であり，これらの素符号の重みの最小値wは，

$$w = \begin{cases} (p^{\alpha} - p^{\alpha-1})(q-1)/3, & (p \equiv 1 (\mathrm{mod}\ 3)) \\ (p^{\alpha} - p^{\alpha-1} - 2p^{\alpha-2})(q-1)/3, & (p \equiv -1 (\mathrm{mod}\ 3)) \end{cases} \qquad (5.158)$$

である．

最後に，$Ap^{\alpha}q \cdot G(2) = (3^{n}-1)/2 = (11\cdots1)_{ST}$であり，この符号語の重みwは，

$$w = n = (p^{\alpha} - p^{\alpha-1})(q-1)/2 \qquad (5.159)$$

である．

以上，式(5.153)～(5.159)により，式(5.152)を得る．　　（証明終）

(3)の場合を考える．このとき，符号長nと生成数Aは，(1),(2)の場合の式(5.142)に一致する．

[定理５.23]　法p^{α}に関して3でなく-3が原始根であり，法qに関して3が原始根であって，$(p^{\alpha}-p^{\alpha-1}, q-1)=2$なら，$B=2p^{\alpha}q$ で規定される符号 I_B の最小距離は，

$$d_m = \begin{cases} (p^{\alpha} - p^{\alpha-1})(q-2)/3, & (q \equiv 1 (\mathrm{mod}\ 3)) \text{または} (q \equiv -1 (\mathrm{mod}\ 3), p<q) \\ (p^{\alpha} - 2p^{\alpha-1})(q-1)/3, & (q \equiv -1 (\mathrm{mod}\ 3), p>q) \end{cases} \qquad (5.159)$$

である．

（証明）　はじめに，部分符号$A \cdot G(2p^{\alpha-i}q)$について考える．$G(2p^{\alpha-i}q)$については，補題５.14が成立し，この部分符号が重みの等しい２個の素符号（式(5.142)）に展開されるため，定理５.21の場合に等しい．法pに関して-3が原始根

であるから，$p \not\equiv 1 \pmod 3$ なることに注意して，これらの素符号の重みの最小値wは，式(5.144)の第１,第２式で与えられる．すなわち，

$$w = \begin{cases} [(p^{\alpha}-p^{\alpha-1})(q-1)-2p^{\alpha-2}]/3, & (q \equiv -1 \pmod 3), \\ (p^{\alpha}-p^{\alpha-1})(q-1)/3, & (q \equiv -1 \pmod 3) \end{cases} \tag{5.160}$$

部分符号$A2p^{i}\cdot G(p^{\alpha-i}q)$を考える．これは，定理５.20の証明における部分符号$Ap^{i}\cdot G(p^{\alpha-i}q)$と同じであり，これらに含まれる素符号の重みの最小値wは，式(5.138)で与えられ，

$$w = \begin{cases} (p^{\alpha}-p^{\alpha-1})(q-1)/3, & (q \equiv 1 \pmod 3) \\ [(p^{\alpha}-p^{\alpha-1})(q-1)-4p^{\alpha-1}]/3, & (q \equiv -1 \pmod 3) \end{cases} \tag{5.161}$$

である．

次に，部分符号$Ap^{i}q\cdot(2p^{\alpha-i})$を考える．これらの素符号の重みの最小値wは，定理５.10の素符号の重み（式(5.54)）の(q-1)倍で与えられ，

$$w = (p^{\alpha}-2p^{\alpha-1})(q-1)/3 \tag{5.162}$$

である．また，部分符号$A2p^{i}q\cdot G(p^{\alpha-i})$についても同様であり，これらの素符号の重みの最小値wは，定理５.８の素符号の最小重み（式(5.41)）の(q-1)倍で与えられ，

$$w = (p^{\alpha}-p^{\alpha-1}-2p^{\alpha-2})(q-1)/3, \quad (p \equiv -1 \pmod 3) \tag{5.163}$$

である．

部分符号$Ap^{\alpha}\cdot G(2q)$については，(1)の場合（式(5.149)）と同様であり，この素符号の重みwは，

$$w = \begin{cases} (p^{\alpha}-p^{\alpha-1})(q-1)/3, & (q \equiv 1 \pmod 3) \\ (p^{\alpha}-p^{\alpha-1})(q-2)/3, & (q \equiv -1 \pmod 3) \end{cases} \tag{5.164}$$

である．また，部分符号$A2p^{\alpha}\cdot G(q)$についても同様であり，この素符号の重みwは式(5.150)により，

$$w_s = \begin{cases} (p^{\alpha} - p^{\alpha-1})(q-1)/3, & (q \equiv 1 (\mathrm{mod}\ 3)) \\ (p^{\alpha} - p^{\alpha-1})(q+1)/3, & (q \equiv -1 (\mathrm{mod}\ 3)) \end{cases} \qquad (5.165)$$

を得る．

最後に，$Ap^{\alpha}q \cdot G(2) = (3^n - 1)/2 = (11\cdots1)_{ST}$であり，この符号語の重みは，

$$w = n = (p^{\alpha} - p^{\alpha-1})(q-1)/2 \qquad (5.166)$$

である．

以上，式(5.160)～(5.166)により，式(5.159)を得る．　　（証明終）

5．8　符号語数$B=p^{\alpha}q^{\beta}$，$2p^{\alpha}q^{\beta}$で規定される符号

(1)　$B=p^{\alpha}q^{\beta}$

p,qは相異なる5以上の素数，α，βは2以上の整数である．法$B=p^{\alpha}q^{\beta}$に関する既約剰余系$G(p^{\alpha}q^{\beta})$の位数は，

$$\varphi(p^{\alpha}q^{\beta}) = (p^{\alpha} - p^{\alpha-1})(q^{\beta} - q^{\beta-1}) \qquad (5.167)$$

である．符号語数$B=p^{\alpha}q^{\beta}$で規定される符号 I_A は，

$$\begin{aligned} I_A = {} & A \cdot G(p^{\alpha}q^{\beta}) + Ap \cdot G(p^{\alpha-1}q^{\beta}) + \cdots + Ap^{\alpha} \cdot G(q^{\beta}) \\ & + Aq \cdot G(p^{\alpha}q^{\beta-1}) + Apq \cdot G(p^{\alpha-1}q^{\beta-1}) + \cdots \\ & \qquad \cdots + Ap^{\alpha}q \cdot G(q^{\beta-1}) \\ & + Aq^{\beta} \cdot G(p^{\alpha}) + Apq^{\beta} \cdot G(p^{\alpha-1}) + \cdots + Ap^{\alpha}q^{\beta} \cdot G(1), \\ & \qquad (G(1) = \{0\}) \qquad (5.168) \end{aligned}$$

のように，$(\alpha+1)(\beta+1)$個の部分符号に分解される．以下では，

(1) 法p^{α},q^{β}に関して3が原始根である場合，

(2) 法p^{α}に関して3が原始根であり，法q^{β}に関して3でなく-3が原始根である場

合，

の２つについて検討する．いずれにしても，法$p^{\alpha}q^{\beta}$に関する原始根は存在しない．

(1)の場合，(h)B=pqの場合と同様，$(p^{\alpha}-p^{\alpha-1},q^{\beta}-p^{\beta-1})=2$ で，$4\mid(p-1)$ または $4\mid(q-1)$なる条件を付け加える．このとき，

$$n = E(3,p^{\alpha}q^{\beta}) = LCM[E(3,p^{\alpha}),E(3,q^{\beta})]$$
$$= (p^{\alpha}-p^{\alpha-1})(q^{\beta}-q^{\beta-1})/2,$$
$$A = (3^{n}-1)/(p^{\alpha}q^{\beta}) \qquad (5.169)$$

である．

[補題５.12]　法p^{α},q^{β}に関して3が原始根であり，$(p^{\alpha}-p^{\alpha-1},q^{\beta}-q^{\beta-1})=2$，しかも，$4\mid(p-1)$または$4\mid(q-1)$ なら，

$$3^{g} \equiv -1 \pmod{p^{\alpha-i}q^{\beta\ j}},\ 3^{g} \equiv -1 \pmod{2p^{\alpha-i}q^{\beta\ j}},$$
$$(0<g<(p^{\alpha-i}-p^{\alpha-i-1})(q^{\beta-j}-q^{\beta\ j-1})/2;$$
$$i=0,1,\cdots,\alpha-1,\ j=0,1,\cdots,\beta-1)) \qquad (5.170)$$

である．

（証明）　付録参照　　（証明終）

定理５.14の場合と同様，補題の条件において，$4\mid(p-1)$ または $4\mid(q-1)$ のどちらか一方が成立する．補題５.２により，-3は法pまたは法qのどちらか一方に関する原始根である．このため，$p\equiv q\equiv 1 \pmod 3$ではあり得ないし，また，$p\equiv q\equiv -1 \pmod 3$でもない．このため，$4\mid(p-1)$であるとする．このため，$p\equiv -q\equiv -1 \pmod 3$であることに注意すれば，以下の定理が得られる．

[定理５.24]　法p^{α},q^{β}に関して3が原始根であって，$(p^{\alpha}-p^{\alpha-1},q^{\beta}-q^{\beta-1})$

=2であり，しかも，4 |(p-1) なら，$B=p^{\alpha}q^{\beta}$ で規定される符号 I_A の最小距離は

$$d_m = (p^{\alpha}-p^{\alpha-1}-2p^{\alpha-2})(q^{\beta}-q^{\beta-1})/3 \qquad (5.171)$$

である．

（証明） はじめに，部分符号$Ap^iq^j\cdot G(p^{\alpha-i}q^{\beta-j})$, (i=0,1,・・・,$\alpha$-1, j=0, 1,・・・,$\beta$-1)を検討する．定理の条件から，

$$\varphi(p^{\alpha-i}q^{\beta-j}) = (p^{\alpha-i}-p^{\alpha-i-1})(q^{\beta-j}-q^{\beta-j-1}),$$

$$E(3,p^{\alpha-i}q^{\beta-j}) = (p^{\alpha-i}-p^{\alpha-i-1})(q^{\beta-j}-q^{\beta-j-1})/2$$

$$= \varphi(p^{\alpha-i}q^{\beta-j})/2 \qquad (5.172)$$

であるから，$G(p^{\alpha-i}q^{\beta-j})$は，2個のコセットに展開され，補題５.15により，この部分符号は，重みの等しい２個の素符号に分解される． 符号長 n が E(3, $p^{\alpha-i}q^{\beta-j}$) のp^iq^j倍であるから，これらの素符号の重みwは，

$$w = p^iq^j \times (1/2) \times \#\{e \mid e\in G(p^{\alpha-i}q^{\beta-j}), (3,e)=1\}$$

で与えられる．$G(p^{\alpha-i}q^{\beta-j})$は，集合

$$S_1=\{\pm k \mid k=1,2,\cdots,(p^{\alpha-i}q^{\beta-j}-1)/2\}$$

から，pの倍数の集合とqの倍数の集合

$$S_2=\{\pm pk \mid k=1,2,\cdots,(p^{\alpha-i-1}q^{\beta-j}-1)/2\},$$

$$S_3=\{\pm qk \mid k=1,2,\cdots,(p^{\alpha-i}q^{\beta-j-1}-1)/2\}$$

を除き，pqの倍数の集合

$$S_4=\{\pm pqk \mid k=1,2,\cdots,(p^{\alpha-i-1}q^{\beta-j-1}-1)/2\}$$

を加えて補正したものである．これら(S_1～S_4)の元のうち，それぞれから3の倍数を除き，残された元の個数それぞれw_1～w_4とすると，これらに属する素符号の重みw(i)は

$$w(i)=p^iq^j(w_1-w_2-w_3+w_4)/2$$

である．このとき，

$$w_1 = \begin{cases} 2(p^{\alpha-i}q^{\beta-j}-1)/3, & (p^{\alpha-i}q^{\beta-j} \equiv 1 (\mathrm{mod}\ 3)) \\ 2(p^{\alpha-i}q^{\beta-j}+1)/3, & (p^{\alpha-i}q^{\beta-j} \equiv -1 (\mathrm{mod}\ 3)) \end{cases}$$

$$w_2 = \begin{cases} 2(p^{\alpha-i-1}q^{\beta-j}-1)/3, & (p^{\alpha-i-1}q^{\beta-j} \equiv 1 (\mathrm{mod}\ 3)) \\ 2(p^{\alpha-i-1}q^{\beta\ \ j}+1)/3, & (p^{\alpha-i-1}q^{\beta-j} \equiv -1 (\mathrm{mod}\ 3)) \end{cases}$$

$$w_3 = \begin{cases} 2(p^{\alpha-i}q^{\beta-j-1}-1)/3, & (p^{\alpha-i}q^{\ \beta-j-1} \equiv 1 (\mathrm{mod}\ 3)) \\ 2(p^{\alpha-i}q^{\beta\ \ j-1}+1)/3, & (p^{\alpha-i}q^{\beta-j-1} \equiv -1 (\mathrm{mod}\ 3)) \end{cases}$$

$$w_4 = \begin{cases} 2(p^{\alpha-i-1}q^{\beta-j-1}-1)/3, & (p^{\alpha\ \ i-1}q^{\beta-j-1} \equiv 1 (\mathrm{mod}\ 3)) \\ 2(p^{\alpha-i-1}q^{\beta-j-1}+1)/3, & (p^{\alpha-i-1}q^{\beta-j-1} \equiv -1 (\mathrm{mod}\ 3)) \end{cases}$$

である．これらの素符号の重みw(i,j)は，

$$w(i,j) = \begin{cases} [(p^{\alpha}-p^{\alpha-1})(q^{\beta}-q^{\beta-1})-4p^{i}q^{j}]/3, \\ \qquad (p \equiv q \equiv -1 (\mathrm{mod}\ 3),\ \alpha-i \equiv \beta-j (\mathrm{mod}\ 2)) \\ [(p^{\alpha}-p^{\alpha-1})(q^{\beta}-q^{\beta-1})+4p^{i}q^{j}]/3, \\ \qquad (p \equiv q \equiv -1 (\mathrm{mod}\ 3),\ \alpha-i \not\equiv \beta-j (\mathrm{mod}\ 2)) \\ (p^{\alpha}-p^{\alpha-1})(q^{\beta}-q^{\beta-1})/3, \text{（その他）} \end{cases}$$

である．w(i,j)の最小値w'は，

$$w' = \begin{cases} [(p^{\alpha}-p^{\alpha-1})(q^{\beta}-q^{\beta-1})-4p^{\alpha-1}q^{\beta-1}]/3, \\ \qquad (p \equiv q \equiv -1 (\mathrm{mod}\ 3)) \\ (p^{\alpha}-p^{\alpha-1})(q^{\beta}-q^{\beta-1})/3, \text{（その他）} \end{cases} \qquad (5.173)$$

である．さらに，定理の条件により，$p \not\equiv q (\mathrm{mod}\ 3)$であるから，これらの部分符号に属する素符号の重みの最小値wは，

$$w = (p^{\alpha}-p^{\alpha-1})(q^{\beta}-q^{\beta-1})/3 \qquad (5.174)$$

である．

次に，部分符号$Ap^{i}q^{\beta} \cdot G(p^{\alpha\ i}),(i=0,1,\cdots,\alpha-1)$を検討する．法$p^{\alpha}$に関して3が原始根であるから，補題５．３により，3は法$p^{\alpha\ i},(i=0,1,\cdots,\alpha-1)$に関しても原始根である．このため，これらの部分符号はそれぞれが強巡回的な素符号

である．これらの素符号の重みw(i)は，

$$w(i) = p^{i}(q^{\beta}-q^{\beta-1})/2 \times \#\{e \mid e\in G(p^{\alpha-i})\}$$

で与えられる．この最小値wは定理５．７の式(5.37)の第２式を利用して，

$$w = (p^{\alpha}-p^{\alpha-1}-2p^{\alpha-2})(q^{\beta}-q^{\beta-1})/3 \qquad (5.175)$$

部分符号$Ap^{\alpha}q^{j}\cdot G(q^{\beta-j})$を考える．これは，上の部分符号と同様にして，求めることができる．これらの素符号の重みの最小値wは，式(5.37)の第１式により，

$$w = (p^{\alpha}-p^{\alpha-1})(q^{\beta}-q^{\beta-1})/3 \qquad (5.176)$$

で与えられる．

以上，式(5.174)～(5.176)により，(5.171)を得る．　　（証明終）

(2)の場合を考える．このとき，符号長nと生成数Aは，(1)の場合の式(5.169)に一致する．

[補題５．16]　法p^{α}に関して3が原始根であり，法q^{β}に関して3でなく-3が原始根であって，$(p^{\alpha}-p^{\alpha-1},q^{\beta}-q^{\beta-1})=2$ なら，

$$3^{g} \equiv -1 \pmod{p^{\alpha-i}q^{\beta-j}},\ 3^{g} \equiv -1 \pmod{2p^{\alpha-i}q^{\beta-j}},$$

$$(0<g<(p^{\alpha-i}-p^{\alpha-i-1})(q-1)/2,\ (i=0,1,\cdots,\alpha-1)) \qquad (5.177)$$

である．

（証明）　補題５．15と同様にして証明される．　　（証明終）

[定理５．25]　法p^{α}に関して3が原始根であり，法q^{β}に関して3でなく-3が原始根であって，$(p^{\alpha}-p^{\alpha-1},q^{\beta}-q^{\beta-1})=2$ なら，$B=p^{\alpha}q^{\beta}$で規定される符号 l_B の最小距離は

$$d_m = \begin{cases} (p^{\alpha}-p^{\alpha-1})(q^{\beta}-q^{\beta-1}-2q^{\beta-2})/3, \\ \quad (p\equiv 1(\mathrm{mod}\ 3))\text{または}(p\equiv -1(\mathrm{mod}\ 3), q<(p-1)/2) \\ [(p^{\alpha}-p^{\alpha-1})(q^{\beta}-q^{\beta-1})-4p^{\alpha-1}q^{\beta-1}]/3, \\ \quad (p\equiv -1(\mathrm{mod}\ 3),\ (p-1)/2<q<2p+1) \\ (p^{\alpha}-p^{\alpha-1}-2p^{\alpha-2})(q^{\beta}-q^{\beta-1})/3, \\ \quad (p\equiv -1(\mathrm{mod}\ 3),\ 2p+1<q) \end{cases} \tag{5.178}$$

である．

（証明） はじめに，部分符号$Ap^iq^j\cdot G(p^{\alpha-i}q^{\beta-j})$，$(i=0,1,\cdots,\alpha-1,\ j=0,1,\cdots,\beta-1)$を検討する．定理の条件から，

$$E(3,p^{\alpha-i}q^{\beta-j}) = (p^{\alpha-i}-p^{\alpha-i-1})(q^{\beta-j}-q^{\beta-j-1})/2$$
$$= \varphi(p^{\alpha-i}q^{\beta\ j})/2$$

であるから，$G(p^{\alpha-i}q^{\beta\ j})$は，前定理と同様，2個のコセットに展開され，補題５.16により，この部分符号は，重みの等しい２個の素符号に分解される．これらの素符号の重みの最小値wは，

$$w = \begin{cases} [(p^{\alpha}-p^{\alpha-1})(q^{\beta}-q^{\beta-1})-4p^{\alpha-1}q^{\beta-1}]/3, \\ \quad (p\equiv q\equiv -1(\mathrm{mod}\ 3)) \\ (p^{\alpha}-p^{\alpha-1})(q^{\beta}-q^{\beta-1})/3,\ (\text{その他}) \end{cases} \tag{5.179}$$

である．

次に部分符号$Ap^iq^{\beta}\cdot G(p^{\alpha-i})$については，前定理の場合と同じであり，定理５.７を用いて，

$$w = \begin{cases} [(p^{\alpha}-p^{\alpha-1})(q^{\beta}-q^{\beta-1})4p^{\alpha-1}q^{\beta-1}]/3, \\ \quad (p\equiv q\equiv -1(\mathrm{mod}\ 3)) \\ (p^{\alpha}-p^{\alpha-1}-2p^{\alpha-2})(q^{\beta}-q^{\beta-1})/3,\ (\text{その他}) \end{cases} \tag{5.180}$$

である．

また，部分符号$Ap^{\alpha}q^j\cdot G(q^{\beta-j})$については，定理５.８の場合と同様であり，

これらの素符号の重みの最小値wは，

$$w = (p^{\alpha} - p^{\alpha-1})(q^{\beta} - q^{\beta-1} - 2q^{\beta-2})/3 \qquad (5.181)$$

で与えられる．

以上，式(5.179)～(5.181)により，(5.178)を得る． （証明終）

(m) $B=2p^{\alpha}q^{\beta}$

法$B=2p^{\alpha}q^{\beta}$に関する既約剰余系$G(2p^{\alpha}q^{\beta})$の位数は，

$$\varphi(2p^{\alpha}q) = (p^{\alpha} - p^{\alpha-1})(q^{\beta} - q^{\beta-1}) \qquad (5.182)$$

である．符号語数$B=2p^{\alpha}q^{\beta}$で規定される符号I_Aは，

$$\begin{aligned}
I_A = {} & A\cdot G(2p^{\alpha}q^{\beta}) + Ap\cdot G(2p^{\alpha-1}q^{\beta}) + \cdots + Ap^{\alpha}\cdot G(2q^{\beta}) \\
& + Aq\cdot G(2p^{\alpha}q^{\beta-1}) + Apq\cdot G(2p^{\alpha-1}q^{\beta-1}) + \cdots \\
& \qquad\qquad \cdots + Ap^{\alpha}q\cdot G(2q^{\beta-1}) \\
& + \cdots\cdots \\
& + Aq^{\beta}\cdot G(2p^{\alpha}) + Apq^{\beta}\cdot G(2p^{\alpha-1}) + \cdots + Ap^{\alpha}q^{\beta}\cdot G(2) \\
& + A2\cdot G(p^{\alpha}q^{\beta}) + A2p\cdot G(p^{\alpha-1}q^{\beta}) + \cdots + A2p^{\alpha}\cdot G(q^{\beta}) \\
& + A2q\cdot G(p^{\alpha}q^{\beta-1}) + A2pq\cdot G(2p^{\alpha-1}q^{\beta-1}) + \cdots \\
& \qquad\qquad \cdots + A2p^{\alpha}q\cdot G(q^{\beta-1}) \\
& + \cdots\cdots \\
& + A2q^{\beta}\cdot G(p^{\alpha}) + A2pq^{\beta}\cdot G(p^{\alpha-1}) + \cdots + A2p^{\alpha}q^{\beta}\cdot G(1), \\
& \qquad\qquad (G(2)=\{1\}, G(1)=\{0\}) \qquad (5.183)
\end{aligned}$$

のように，$2(\alpha+1)(\beta+1)$個の部分符号に分解される．以下では，(1)と同様，

(1) 法p^{α}, q^{β}に関して3が原始根である場合，

(2) 法p^{α}に関して3が原始根であり，法q^{β}に関して3でなく-3が原始根である場合，

の２つについて検討する．いずれにしても，法$2p^{\alpha}q^{\beta}$に関する原始根は存在しない．

(1)の場合，(i)B=2pqの場合と同様，$(p^{\alpha}-p^{\alpha-1},q^{\beta}-q^{\beta-1})=2$ で，$4\mid(p-1)$ または $4\mid(q-1)$なる条件を付け加える．このとき，

$$n = E(3,2p^{\alpha}q^{\beta}) = (p^{\alpha}-p^{\alpha-1})(q^{\beta}-q^{\beta-1})/2$$
$$= \varphi(2p^{\alpha}q^{\beta})/2,$$
$$A = (3^{n}-1)/(2p^{\alpha}q^{\beta}) \qquad (5.184)$$

である．

[定理５.26] 法p^{α},q^{β}に関して3が原始根であって，$(p^{\alpha}-p^{\alpha-1},q^{\beta}-q^{\beta-1})=2$であって，しかも，$4\mid(p-1)$ なら，$B=2p^{\alpha}q^{\beta}$で規定される符号 l_A の最小距離は

$$d_m = (p^{\alpha}-2p^{\alpha-1})(q^{\beta}-q^{\beta-1})/3 \qquad (5.185)$$

である．

（証明） はじめに，部分符号$Ap^{i}q^{j}\cdot G(2p^{\alpha-i}q^{\beta-j})$, $(i=0,1,\cdots,\alpha-1;j=0,1,\cdots,\beta-1)$を考える．定理の条件と補題５.15により，この部分符号は重みの等しい２個の素符号に展開される．$G(2p^{\alpha-i}q^{\beta\ j})$は，集合

$$S_1=\{\pm k \mid k=1,2,\cdots,p^{\alpha-i}q^{\beta-j}\}$$

から，2,p,qの各々の倍数の集合

$$S_2=\{\pm 2k \mid k=1,2,\cdots,(p^{\alpha-i}q^{\beta-j}-1)/2\},$$
$$S_3=\{\pm pk \mid k=1,2,\cdots,p^{\alpha-i-1}q^{\beta-j}\}$$
$$S_4=\{\pm qk \mid k=1,2,\cdots,p^{\alpha\ i}q^{\beta-j-1}\}$$

を除き，2p,pq,2qの倍数の集合

$$S_5=\{\pm 2pk \mid k=1,2,\cdots,(p^{\alpha-i-1}q^{\beta\ j}-1)/2\}$$

$$S_6=\{\pm pqk \mid k=1,2,\cdots,p^{\alpha-i-1}q^{\beta\ j-1}\}$$

$$S_7=\{\pm 2qk \mid k=1,2,\cdots,(p^{\alpha-i}q^{\beta-j-1}-1)/2\}$$

を加え，さらに，2pqの倍数の集合

$$S_8=\{\pm 2pqk \mid k=1,2,\cdots,(p^{\alpha-i-1}q^{\beta-j-1}-1)/2\}$$

を除いて補正したものである．集合S_1～S_8の各々から3の倍数を除いて残った元の個数をそれぞれw_1～w_8とすれば，

$$w_1=\begin{cases}2(2p^{\alpha-i}q^{\beta-j}+1)/3, & (p^{\alpha-i}q^{\beta-j}\equiv 1(\mathrm{mod}\ 3)),\\ 4(p^{\alpha-i}q^{\beta-j}+1)/3, & (p^{\alpha-i}q^{\beta-j}\equiv -1(\mathrm{mod}\ 3))\end{cases}$$

$$w_2=\begin{cases}2(p^{\alpha-i}q^{\beta-j}-1)/3, & (p^{\alpha-i}q^{\beta\ j}\equiv 1(\mathrm{mod}\ 3)),\\ 2(p^{\alpha-i}q^{\beta-j}+1)/3, & (p^{\alpha-i}q^{\beta-j}\equiv -1(\mathrm{mod}\ 3))\end{cases}$$

$$w_3=\begin{cases}2(2p^{\alpha-i-1}q^{\beta-j}+1)/3, & (p^{\alpha-i-1}q^{\beta-j}\equiv 1(\mathrm{mod}\ 3)),\\ 4(p^{\alpha-i-1}q^{\beta-j}+1)/3, & (p^{\alpha-i-1}q^{\beta-j}\equiv -1(\mathrm{mod}\ 3))\end{cases}$$

$$w_4=\begin{cases}2(2p^{\alpha-i}q^{\beta-j-1}+1)/3, & (p^{\alpha-i}q^{\beta-j-1}\equiv 1(\mathrm{mod}\ 3)),\\ 4(p^{\alpha-i}q^{\beta\ j-1}+1)/3, & (p^{\alpha-i}q^{\beta\ j-1}\equiv -1(\mathrm{mod}\ 3))\end{cases}$$

$$w_5=\begin{cases}2(2p^{\alpha-i-1}q^{\beta\ j}-1)/3, & (p^{\alpha-i-1}q^{\beta\ j}\equiv 1(\mathrm{mod}\ 3)),\\ 2(2p^{\alpha-i-1}q^{\beta\ j}+1)/3, & (p^{\alpha-i-1}q^{\beta-j}\equiv -1(\mathrm{mod}\ 3))\end{cases}$$

$$w_6=\begin{cases}2(2p^{\alpha-i-1}q^{\beta-j-1}+1)/3, & (p^{\alpha-i-1}q^{\beta-j-1}\equiv 1(\mathrm{mod}\ 3)),\\ 4(p^{\alpha-i-1}q^{\beta-j-1}+1)/3, & (p^{\alpha-i-1}q^{\beta\ j-1}\equiv -1(\mathrm{mod}\ 3))\end{cases}$$

$$w_7=\begin{cases}2(p^{\alpha-i}q^{\beta-j-1}-1)/3, & (p^{\alpha-i}q^{\beta-j-1}\equiv 1(\mathrm{mod}\ 3)),\\ 2(p^{\alpha\ i}q^{\beta-j-1}+1)/3, & (p^{\alpha-i}q^{\beta-j-1}\equiv -1(\mathrm{mod}\ 3))\end{cases}$$

$$w_8=\begin{cases}2(p^{\alpha-i-1}q^{\beta-j-1}-1)/3, & (p^{\alpha-i-1}q^{\beta-j-1}\equiv 1(\mathrm{mod}\ 3)),\\ 2(p^{\alpha-i\ 1}q^{\beta\ j-1}+1)/3, & (p^{\alpha-i-1}q^{\beta-j-1}\equiv -1(\mathrm{mod}\ 3))\end{cases}$$

である．これらに属する素符号の重み$w(i,j)$は

$$w(i,j) = p^i q^j \times (1/2) \times \#\{e \mid e \in G(2p^\alpha q), (3,e)=1\}$$

$$= (p^i q^j/2) \times (w_1 - w_2 - w_3 - w_4 + w_5 + w_6 + w_7 - w_8)$$

$$= \begin{cases} [(p^\alpha - p^{\alpha-1})(q^\beta - q^{\beta-1}) + 2p^i q^j]/3, \\ \qquad (p \equiv q \equiv -1 \pmod 3),\ \alpha - i \equiv \beta - j \pmod 2) \\ [(p^\alpha - p^{\alpha-1})(q^\beta - q^{\beta-1}) - 2p^i q^j]/3, \\ \qquad (p \equiv q \equiv -1 \pmod 3),\ \alpha - i \not\equiv \beta - j \pmod 2) \\ (p^\alpha - p^{\alpha-1})(q^\beta - q^{\beta-1})/3, \quad (\text{その他}) \end{cases}$$

である．w(i,j)の最小値w'は，

$$w' = \begin{cases} [(p^\alpha - p^{\alpha-1})(q^\beta - q^{\beta-1}) - 2p^{\alpha-1} q^{\beta-2}]/3, \\ \qquad (p \equiv q \equiv -1 \pmod 3), p > q) \\ (p^\alpha - p^{\alpha-1})(q^\beta - q^{\beta-1})/3, (\text{その他}) \end{cases} \qquad (5.186)$$

である．さらに，定理の条件により，$p \not\equiv 1, q \pmod 3$であるから，これらの部分符号に属する素符号の重みの最小値wは，

$$w = (p^\alpha - p^{\alpha-1})(q^\beta - q^{\beta-1})/3 \qquad (5.187)$$

である．

次に，部分符号$A2p^i q^j \cdot G(p^{\alpha-i} q^{\beta\ j})$は定理５.24の部分符号と同じであり，これらに含まれる素符号の重みの最小値wは

$$w = (p^\alpha - p^{\alpha\ 1})(q^\beta - q^{\beta-1})/3 \qquad (5.188)$$

である．

次に，部分符号$Ap^i q^\beta \cdot G(2p^{\alpha-i})$を考える．これは，定理５.９の部分符号と同様である．これらに含まれる素符号の重みの最小値wは，

$$w = (p^\alpha - 2p^{\alpha-1})(q^\beta - q^{\beta-1})/3 \qquad (5.189)$$

である．同様にして，部分符号$Ap^\alpha q^j \cdot G(2q^{\beta-j})$に含まれる素符号の重みの最小値wは，

$$w = (p^\alpha - p^{\alpha-1})(q^\beta - q^{\beta-1})/3 \qquad (5.190)$$

である．

次に，部分符号$A2p^{i}q\cdot G(p^{\alpha-i})$は定理５．24の部分符号$Ap^{i}q\cdot G(p^{\alpha-i})$と同じであり，これらの素符号の最小重みwは，

$$w = (p^{\alpha}-p^{\alpha-1}-2p^{\alpha-2})(q^{\beta}-q^{\beta-1})/3 \qquad (5.191)$$

である．同様にして，部分符号$A2p^{\alpha}q^{j}\cdot G(q^{\beta\ j})$の素符号の重みの最小値wは，

$$w = (p^{\alpha}-p^{\alpha-1})(q^{\beta}-q^{\beta-1})/3 \qquad (5.192)$$

で与えられる．

以上，式(5.187)～(5.192)により，式(5.185)を得る．　　（証明終）

(2)の場合を考える．このとき，符号長nと生成数Aは，(1)の場合の式(5.169)に一致する．

[定理５．27]　法p^{α}に関して3が原始根であり，法q^{β}に関して3でなく-3が原始根であって，$(p^{\alpha}-p^{\alpha-1},q^{\beta}-q^{\beta-1})=2$ なら，$B=p^{\alpha}q^{\beta}$で規定される符号 l_B の最小距離は

$$d_m = \begin{cases} (p^{\alpha}-p^{\alpha-1})(q^{\beta}-2q^{\beta-1})/3, \\ \qquad (p\equiv 1(\mathrm{mod}\ 3))\text{または}(p\equiv -1(\mathrm{mod}\ 3), p<q) \\ (p^{\alpha}-2p^{\alpha-1})(q^{\beta}-q^{\beta-1})/3, \\ \qquad (p\equiv -1(\mathrm{mod}\ 3), p>q) \end{cases} \qquad (5.193)$$

である．

（証明）はじめに，部分符号$Ap^{i}q^{j}\cdot G(2p^{\alpha-i}q^{\beta-j})$，$(i=0,1,\cdots,\alpha-1,\ j=0,1,\cdots,\beta\ 1)$を検討する．定理の条件から，

$$E(3.2p^{\alpha-i}q^{\beta-j}) = (p^{\alpha-i}-p^{\alpha-i-1})(q^{\beta\ j}-q^{\beta\ j-1})/2$$
$$= \varphi(2p^{\alpha-i}q^{\beta\ j})/2$$

であるから，$G(2p^{\alpha-i}q^{\beta-j})$は，前定理の場合と同様，2個のコセットに展開され，補題５．16により，この部分符号は，重みの等しい２個の素符号に分解される．

これらの素符号の重みの最小値wは，

$$w = \begin{cases} [(p^{\alpha}-p^{\alpha-1})(q^{\beta}-q^{\beta-1})-2p^{\alpha-1}q^{\beta-2}]/3, \\ \qquad (p\equiv q\equiv -1(\mathrm{mod}\ 3), p>q) \\ (p^{\alpha}-p^{\alpha-1})(q^{\beta}-q^{\beta-1})/3, \text{（その他）} \end{cases} \tag{5.194}$$

である．また，部分符号$A2p^{i}q^{j}\cdot G(p^{\alpha-i}q^{\beta-j})$は定理５.25と同じである．これらの素符号の重みの最小値wは，

$$w = \begin{cases} [(p^{\alpha}-p^{\alpha-1})(q^{\beta}-q^{\beta-1})-4p^{\alpha-1}q^{\beta-1}]/3, \\ \qquad (p\equiv q\equiv -1(\mathrm{mod}\ 3)) \\ (p^{\alpha}-p^{\alpha-1})(q^{\beta}-q^{\beta-1})/3, \text{（その他）} \end{cases} \tag{5.195}$$

である．

次に，部分符号$Ap^{i}q^{\beta}\cdot G(2p^{\alpha-i})$は前定理の場合と同じであり，これらの素符号の重みの最小値wは

$$w = \begin{cases} (p^{\alpha}-p^{\alpha-1})(q^{\beta}-q^{\beta-1})/3, \ (p\equiv 1(\mathrm{mod}\ 3)) \\ (p^{\alpha}-2p^{\alpha-1})(q^{\beta}-q^{\beta-1})/3, \ (p\equiv -1(\mathrm{mod}\ 3)) \end{cases} \tag{5.196}$$

で与えられる．同様に，部分符号$A2p^{i}q\cdot G(p^{\alpha-i})$についても前定理の場合と同じであり，これらの素符号の最小重みwは，

$$w = (p^{\alpha}-p^{\alpha-1}-2p^{\alpha-2})(q^{\beta}-q^{\beta-1})/3 \tag{5.197}$$

部分符号$Ap^{\alpha}q^{j}\cdot G(2q^{\beta\ j})$は，定理５.10の場合と同様にして，これらに含まれる素符号の重みの最小値wは，

$$w = (p^{\alpha}-p^{\alpha-1})(q^{\beta}-2q^{\beta-1})/3 \tag{5.198}$$

で与えられる．また，部分符号$Ap^{\alpha}q^{j}\cdot G(q^{\beta-j})$については，定理５.８の場合と同様であり，これらの素符号の重みの最小値wは，

$$w = (p^{\alpha}-p^{\alpha-1})(q^{\beta}-q^{\beta-1}-2q^{\beta-2})/3 \tag{5.199}$$

で与えられる．

以上，式(5.193)～(5.199)により，(5.193)を得る．　（証明終）

５．９　最小距離算定結果のまとめ

符号語数Bにより，最小距離の算定公式（５．３節～５．８節）が与えられた符号について検討する．そこに示した定理（定理５．１～５.27）はBに対する条件が複数個組み合わされた形であるため，各定理に関する符号またはその最小距離の算定公式を簡単のため記号（(a)～(m')）で呼ぶことにする．ここに，英小文字の右肩についている ' や " はBの素因数の型の２番目，３番目の定理に関するものである．図５.１において，これらの符号の符号語数Bと最小距離d_mの関係を示す．

これらの符号の符号長nはG(B)の位数φ(B)またはφ(B)／2で与えられるものである．このような符号は，符号語数に対して最大符号長またはそれに次ぐ符号長を持つものである．これらはその部分符号の全てが１個か２個の素符号からなり，２個の素符号からなる場合にはさらに両素符号の重みが等しい場合である．したがって，このような符号は，符号語数Bに対する最小距離の値d_m/Bの限界値2/3またはそれに準じる大きな値を持つものである．図５.１において，これらの符号は，d_m/Bのとる値によって４本の直線（d_m/B = 2/3, 1/3, 1/6, 1/8）上の付近に分かれて位置する．それぞれのd_m/Bにより，以下の符号が対応する．

2/3 ≒(a), (d)

1/3 ≒(a'), (b),(d'),(e),(h),(h'),(j),(j'),(j"),(l),(l')

1/6 ≒(b'), (c),(c'),(e'),(f),(f'),(i),(i'),(k),(k'),(k"),(m),(m')

1/8 = (g)

また，図５.１の各点 ○，△，□，●印はそれぞれ，(a)，(a')，(b')，(g)型符号の実際の最小距離を示す．

符号語数Bが2のべき乗で表される(g)型符号は，Bの丁度1/8，符号長nの丁度半分の最小距離をもつものである．符号長に対する最小距離の値d_m/nは，この(g)型を除いて，すべて$d_m/n \fallingdotseq 2/3$であり，これは，実際に存在する符号の最小距離の限界を示すものである．

５．10　結　言

本章では，符号語数Bが特定の条件を満たす素因数のべき乗やあるいはそれらの積の形で表されるもので，そのようなBで規定される巡回ＳＴ－ＡＮ符号の最小距離をその条件の範囲内で一般的に算定する公式を多数導いた．このような符号の一部は，2進の多重誤り訂正可能な符号[23]に対応するものであり，対応する算定公式は巡回ＳＴ－ＡＮ符号の誤り訂正能力の具体的な限界値を与えるものである．残りの符号についてもその最小距離は巡回ＳＴ－ＡＮ符号の最小距離の限界に近い値である．

本章で公式の得られなかった符号の最小距離は，５．２節で述べた一般的な方法を用いて算定することができる．これは電子計算機プログラムによって容易に実現可能である．

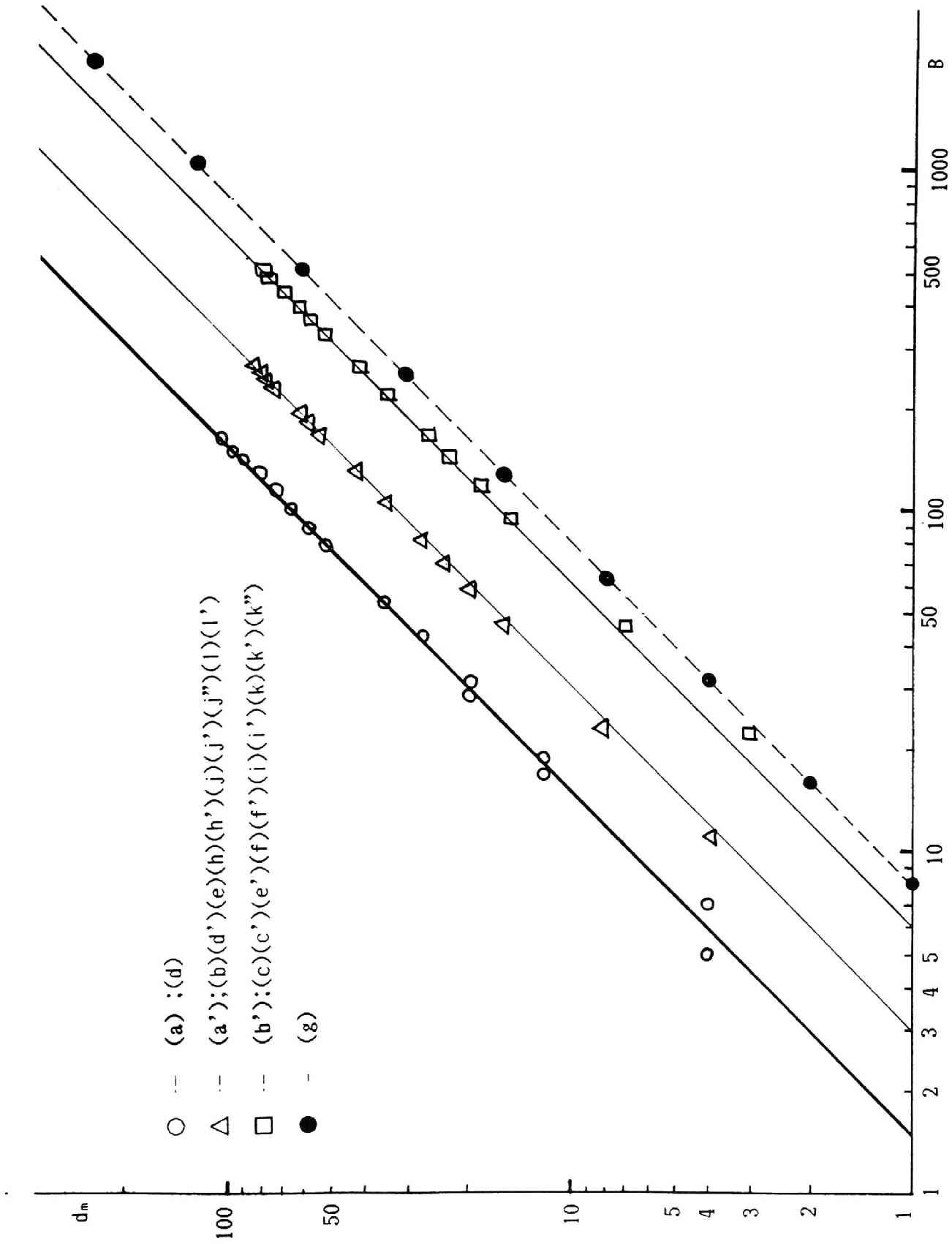

図５．１　定理５．１～５．27のBで規定される巡回ＳＴ－ＡＮ符号の最小距離

表５．１　定理５．１，５．３，５．５の巡回ＳＴ－ＡＮ符号の例（pが5以上の素数で，法pに関して3が原始根であるとき，符号語数B=p,2p,4pで規定される符号の最小距離）

素数	符号長	巡回ＳＴ－ＡＮ符号の最小距離d_m		
p	n=p-1	B=pの場合	B=2pの場合	B=4pの場合
* 5 ≡-1(mod 3)	4	4	2	2
7 ≡ 1(mod 3)	6	4	4	
*17 ≡-1(mod 3)	16	12	10	10
19 ≡ 1(mod 3)	18	12	12	
*29 ≡-1(mod 3)	28	20	18	18
31 ≡ 1(mod 3)	30	20	20	
43 ≡ 1(mod 3)	42	28	28	
*53 ≡-1(mod 3)	52	36	34	34
79 ≡ 1(mod 3)	78	52	52	
*89 ≡-1(mod 3)	88	60	58	58

* は定理５．５の条件 4 |(p-1) を満たす素数p.

表５．２　定理５．２，５．４，５．６の巡回ＳＴ－ＡＮ符号の例（pが5以上の素数で，法pに関して3でなく-3が原始根であるとき，符号語数B=p,2p,4pで規定される符号の最小距離）

素数	巡回ＳＴ－ＡＮ符号の符号長 n と 最小距離 d_m					
	B=pの場合		B=2pの場合		B=4pの場合	
p	n=(p-1)/2	d_m	n=(p-1)/2	d_m	n=p-1	d_m
11 ≡-1(mod 3)	5	4	5	3	10	6
23 ≡-1(mod 3)	11	8	11	7	22	14
47 ≡-1(mod 3)	23	16	23	15	46	30
59 ≡-1(mod 3)	29	20	29	19	58	38
71 ≡-1(mod 3)	35	24	35	23	70	46
83 ≡-1(mod 3)	41	28	41	27	82	54

5-A.　付録；補題の証明

（補題５．１の証明）　対偶を証明する．5以上の素数pに対して，$p \equiv 1 \pmod 3$ なら，法pに関して-3が平方剰余であることを示す．Legendreの記号とその性質を使えば，

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)$$

$$= (-1)^{(p-1)/2} \times (-1)^{(p-1)/2 \times (3-1)/2} \left(\frac{p}{3}\right) = \left(\frac{p}{3}\right)$$

$p \equiv 1 \pmod 3$ であるから，

$$\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1,$$

すなわち，-3は法pに関する平方剰余である．このため，

$$x^2 \equiv -3 \pmod p$$

なる数xが存在し，

$$(-3)^{\varphi(p)/2} \equiv x^{\varphi(p)} \equiv 1 \pmod p,$$

すなわち，法pに関して-3が属するべき数は $\varphi(p)/2 = (p-1)/2$ 以下であって，-3は原始根でありえない．　（証明終）

（補題５．２の証明）　±3がともに法pに関する原始根なら，どちらも法pに関する平方剰余でなく，

$$\left(\frac{3}{p}\right) = -1,$$

$$\left(\frac{-3}{p}\right) = (-1)^{(p-1)/2} \left(\frac{3}{p}\right) = -(-1)^{(p-1)/2} = -1$$

であり，

$$(-1)^{(p-1)/2} = 1$$

である．したがって，(p-1)/2は偶数である．-3(または3)が法pに関する原始根なら，補題３．２，３．３により，法pに関して3(または-3)が属するべき数は $\varphi(p)$ か $\varphi(p)/2$ である．後者の場合，補題３．３により，$\varphi(p)/2 = (p-1)/2$ が奇数である．

これは，条件4 |(p-1)に反する．このため，3(または-3)も法pに関して原始根でなければならない．　　（証明終）

（補題５．３の証明） 法$p^{\alpha-1}$に関して3が原始根であることを示せば十分である．法$p^{\alpha-1}$に関して3が属するべき数を$E(3,p^{\alpha-1})$とすると，

$$3^{E(3,p^{\alpha-1})} = kp^{\alpha-1}+1$$

であり，両辺をp乗して，

$$\begin{aligned} 3^{pE(3,p^{\alpha-1})} &= (kp^{\alpha-1}+1)^p \\ &= 1+\binom{p}{1}kp^{\alpha-1}+\binom{p}{2}(kp^{\alpha-1})^2+\cdots+\binom{p}{p}(kp^{\alpha-1})^p \\ &\equiv 1 \pmod{p^{\alpha}} \end{aligned}$$

となる．したがって，$E(3,p^{\alpha})=p^{\alpha}-p^{\alpha-1}$は $pE(3,p^{\alpha-1})$を，すなわち，$p^{\alpha-1}-p^{\alpha-2}$は$E(3,p^{\alpha-1})$を整除する．他方，$E(3,p^{\alpha-1})$は$\varphi(p^{\alpha-1})=p^{\alpha-1}-p^{\alpha-2}$を整除する．このため，

$$E(3,p^{\alpha-1}) = p^{\alpha-1}-p^{\alpha-2} = \varphi(p^{\alpha-1})$$

であり，さらに，一般に，

$$E(3,p^{\alpha-i}) = p^{\alpha-i}-p^{\alpha-i-1} = \varphi(p^{\alpha-i}),\ (i=0,1,\cdots,\alpha-1)$$

が成立する．-3が原始根の場合についても，同様である．　　（証明終）

（補題５．４の証明） i=0の場合は，補題３．３により明らかである．以下，i=1の場合について証明すれば十分である．

$$3^{E(3,p^{\alpha})} = kp^{\alpha}+1 \equiv 1 \pmod{p^{\alpha-1}}$$

なる正整数kが存在する．このため，法$p^{\alpha-1}$に関して3が属するべき数$E(3,p^{\alpha-1})$は$E(3,p^{\alpha})$を整除し，$E(3,p^{\alpha})=k'E(3,p^{\alpha-1})$なる正整数k'が存在する．さらに，

$$3^{E(3,p^{\alpha-1})} = mp^{\alpha-1}+1$$

なる正整数mが存在し，

$$3^{pE(3,p^{\alpha-1})} = (mp^{\alpha-1}+1)^p \equiv 1 \pmod{p^{\alpha}}$$

であるから，$E(3,p^{\alpha})$は$pE(3,p^{\alpha-1})$を整除し，$pE(3,p^{\alpha-1})=m'E(3,p^{\alpha})$なる正整数m'が存在する．このため，

$$pE(3,p^{\alpha-1}) = m'E(3,p^{\alpha}) = k'm'E(3,p^{\alpha-1})$$

であり，さらに，pが素数であるから，k'=1,m'=pであるか，k'=p,m'=1，すなわち，

$$E(3,p^{\alpha-1}) = E(3,p^{\alpha}) \text{ or } (1/p)E(3,p^{\alpha})$$

である．$E(3,p^{\alpha-1})$は$\varphi(p^{\alpha-1}) = p^{\alpha-1}-p^{\alpha-2}$を整除し，$E(3,p^{\alpha})=(p^{\alpha}-p^{\alpha-1})/2>\varphi(p^{\alpha-1})$であるから，

$$E(3,p^{\alpha-1}) = (1/p)E(3,p^{\alpha}) = (p^{\alpha-1}-p^{\alpha-2})/2$$
$$= \varphi(p^{\alpha-1})/2$$

である．$E(3,p^{\alpha}) = p^{\alpha-1}(p-1)/2$が奇数であるから，$E(3,p^{\alpha-1}) = p^{\alpha-1}(p-1)/2$が奇数であることは明らかである．　（証明終）

（補題５．５の証明）　法p^{α}に関して3が原始根であり，$E(3,p^{\alpha})=\varphi(p^{\alpha})=p^{\alpha}-p^{\alpha-1}$とする．

$$3^{E(3,p^{\alpha})}-1 = k(2p^{\alpha}) \equiv 0 \pmod{2p^{\alpha}}$$

なる正整数kが存在する．したがって，$E(3,p^{\alpha})=p^{\alpha}-p^{\alpha-1}$は，$E(3,2p^{\alpha})$を整除する．同時に，$E(3,2p^{\alpha})$は，$\varphi(2p^{\alpha})=p^{\alpha}-p^{\alpha-1}$を整除するから，

$$E(3,2p^{\alpha}) = p^{\alpha}-p^{\alpha-1} = \varphi(p^{\alpha})$$

である．

逆に，法2p　に関して3が原始根であるとする．このとき，

$$3^{E(3,p^{\alpha})} = mp^{\alpha}+1$$

なる正整数mが存在し，$3^{E(3,p^{\alpha})}$が奇数であるから，mは偶数であり，m=2m'なる正整数m'が存在する．このため，

$$3^{E(3,p^{\alpha})}-1 = m'(2p^{\alpha}) \equiv 0 \pmod{2p^{\alpha}}$$

であり，$E(3,2p^{\alpha})=p^{\alpha}-p^{\alpha-1}$は$E(3,p^{\alpha})$を整除する．同時に，$E(3,p^{\alpha})$は$\varphi(p^{\alpha})=p^{\alpha}-p^{\alpha-1}$を整除するから，$E(3,p^{\alpha})=p^{\alpha}-p^{\alpha-1}=\varphi(p^{\alpha})$である．

また，補題５．３により，3は法$p^{\alpha-i}$に関する原始根である．したがって，

$$E(3,2p^{\alpha-i}) = LCM\{E(3,2),E(3,p^{\alpha-i})\}$$
$$= E(3,p^{\alpha-i}) = p^{\alpha-i}-p^{\alpha-i-1} = \varphi(p^{\alpha-i})$$

であり，3は法$2p^{\alpha-i}$に関して原始根である．-3が原始根の場合についても同様である．　　（証明終）

（補題５．６の証明）　$3^{g}+1\equiv 0 \pmod{4p^{\alpha-i}}$,$(0<g<p^{\alpha\ i}-p^{\alpha-i-1})$なら，

$$3^{g}+1 \equiv 0 \pmod 4$$
$$\equiv 0 \pmod{p^{\alpha-i}} \qquad (a.1)$$

である．このとき，$3^{2g}\equiv 1 \pmod{4p^{\alpha-i}}$であるから，$E(3,4p^{\alpha-i})=p^{\alpha-i}-p^{\alpha-i-1}$は2gを整除し，$2g=m(p^{\alpha-i}-p^{\alpha-i-1})$なる正整数mが存在する．このため，

$$0 < 2g = m(p^{\alpha-i}-p^{\alpha-i-1}) < 2(p^{\alpha-i}-p^{\alpha-i-1}),$$
$$m = 1,\ g = p^{\alpha-i-1}(p-1)/2$$

である．仮定により，$4 \mid (p-1)$であるから，$g=2\times p^{\alpha-i-1}(p-1)/2$は偶数であり，$E(3,4)=2$の倍数である．このため，$3^{g}\equiv 1 \pmod 4$となり，式(a.1)に矛盾する．

（証明終）

（補題５.７の証明） $3^g \equiv -1 \pmod{4p^{\alpha-i}}$, $(g<g<p^{\alpha-i}-p^{\alpha-i-1})$なる正整数gを仮定する．このとき，

$$3^g+1 \equiv 0 \pmod{4p^{\alpha-i}} \equiv 0 \pmod{4} \equiv 0 \pmod{p^{\alpha-i}},$$

$$3^{2g} \equiv 1 \pmod{4p^{\alpha-i}} \qquad \text{(a.2)}$$

である．したがって，$E(3,4p^{\alpha-i})$は2gを整除し，$2g=k(p^{\alpha-i}-p^{\alpha-i-1})$なる正整数kが存在する．このため，

$$0 < 2g = k(p^{\alpha-i}-p^{\alpha-i-1}) < 2(p^{\alpha-i}-p^{\alpha-i-1}),$$

$$k = 1,$$

$$g = (p^{\alpha-i}-p^{\alpha-i-1})/2 = E(3,p^{\alpha-i})$$

である．これは，式(a.2)の$3^g+1\equiv0(\mathrm{mod}\ p^{\alpha-i})$に矛盾する．　　（証明終）

（補題５.10の証明） $3^g\equiv1(\mathrm{mod}\ pq)$ を仮定すると，

$$3^g + 1 \equiv 0 \pmod{p}$$

$$\equiv 0 \pmod{q} \qquad \text{(a.3)}$$

であり，$3^{2g}\equiv1(\mathrm{mod}\ pq)$ である．したがって，$E(3,pq)=(p-1)(q-1)/2$ は2gを整除し，$2g=k(p-1)(q-1)/2$なる整数kが存在する．このとき，

$$0 < 2g = k(p-1)(q-1)/2 < (p-1)(q-1),$$

$$k=1,\ g=(p-1)(q-1)/4$$

である．4がp-1またはq-1を整除するなら，gは$E(3,q)=q-1$または$E(3,p)=p-1$の倍数であって，式(a.3)に矛盾する．式(5.89)の第２式も同様にして証明できる．

（証明終）

（補題５.11の証明） $3^g\equiv1(\mathrm{mod}\ pq)$ を仮定すると，

$$3^g + 1 \equiv 0 \pmod{p}$$

$$\equiv 0 \pmod{q} \qquad \text{(a.4)}$$

であり，$3^{2g} \equiv 1 (\mathrm{mod}\ pq)$ である．したがって，$E(3,pq)=(p-1)(q-1)/2$ は2gを整除し，$2g=k(p-1)(q-1)/2$なる整数kが存在する．このとき，

$$0 < 2g = k(p-1)(q-1)/2 < (p-1)(q-1),$$

$$k=1,\ g=(p-1)(q-1)/4$$

である．このgは $E(3,q)=(q-1)/2$ の倍数であって，$3^g \equiv 1 (\mathrm{mod}\ q)$ となり，式(a.4)に矛盾する．式(5.97)の第２式も同様にして証明できる．　　（証明終）

（補題５.15の証明）　$3^g \not\equiv -1 (\mathrm{mod}\ p^{\alpha-i}q^{\beta\ j})$を仮定すると，

$$3^g+1 \equiv 0 (\mathrm{mod}\ p^{\alpha-i}) \equiv (\mathrm{mod}\ q^{\beta-j}), \qquad (a.5)$$

$$3^{2g} \equiv 1 (\mathrm{mod}\ p^{\alpha-i}q^{\beta-j})$$

であるから，$E(3,p^{\alpha-i}q^{\beta-j})=(p^{\alpha-i}-p^{\alpha-i-1})(q^{\beta-j}q^{\beta-j-1})/2$ は2gを整除する．このため，

$$g = (p^{\alpha-i}-p^{\alpha-i-1})(q^{\beta-j}q^{\beta-j-1})/4$$

であるが，$4 \mid (p-1)$ または $4 \mid (q-1)$ であるから，gは$E(3,q^{\beta-j})=(q^{\beta-j}-q^{\beta-j-1})$ または $E(3,p^{\alpha-i})=p^{\alpha-i}-p^{\beta\ j-1})$の倍数である．したがって，$3^g \equiv 1(\mathrm{mod}\ q^{\beta-j})$ または $3^g \equiv 1(\mathrm{mod}\ p^{\alpha-i})$ であって，式(a.5)に矛盾する．また，式(5.170)の第２式も同様にして証明できる．　　（証明終）

第６章　　負巡回ＳＴ－ＡＮ符号

６．１　緒　言

第３章で述べた一般のＳＴ－ＡＮ符号の中には，巡回ＳＴ－ＡＮ符号ではないが，生成数と符号語数との積が3^n+1の形で表される負巡回ＳＴ－ＡＮ符号が存在する．まず，法3^n+1に関する演算と負巡回けた移動を定義し，このような符号に対して，法3^n+1に関するモジュラ距離を導入し，この符号の基礎理論を述べる．同時に，巡回ＳＴ－ＡＮ符号との関係についても述べる．これに基づき，第５章の巡回ＳＴ－ＡＮ符号の最小距離に関する結果を利用して，負巡回ＳＴ－ＡＮ符号の最小距離を算定する公式を示す．前章で述べた巡回ＳＴ－ＡＮ符号の符号長 n と区別するため，以下に述べる符号の符号長を h で表すことにする．

６．２　負巡回けた移動と負巡回ＳＴ－ＡＮ符号

はじめに，ST表現hけた上において，法3^h+1に関する加算を検討しておく．２整数N_1とN_2の法3^h+1に関する加算は，算術加算N_1+N_2の法3^h+1に関する絶対最小剰余，すなわち，

$$(N_1+N_2) \bmod (3^h+1)$$

である．このとき，算術加算N_1+N_2は高々(h+1)けたで表され，整数商Q(=0 または ±1)が存在して，法3^h+1に関する加算は，

$$(N_1+N_2) \bmod (3^h+1) = N_1+N_2-(3^h+1)Q$$

である．

hけたのST表現で表すことができる整数Ｎの範囲は，

$$-\frac{3^h+1}{2} < N < \frac{3^h+1}{2} \qquad (6.1)$$

である．ST表現hけた上でこの加算を実現する場合，算術加算による最高位のけた

(3^{h-1}のけた)からのけた上げがあれば，これの正負の符号を置き換えたものを最下位のけたに加えることにより実行される(図６．１)．これは，法3^h-1に関する加算における循環けた上げに対応するものであり，負循環けた上げということにする．ただし，

$$(N_1 + N_2) \bmod (3^h+1) = \pm(3^h+1)/2$$

の場合，これをhけたで表現することができない．このため，負循環けた上げが実行されるが，これによって，また，新たな負循環けた上げを生むという不都合を生じる．すなわち，ST表現hけた上で，$(\bar{1}\bar{1}\cdots\bar{1})_{ST}$と$(11\cdots1)_{ST}$が限りなく繰り返され，加算が完了されない．これを避けるため，これらを$(00\cdots0)_{ST}$に置数するなどの特別な措置を必要とする．このようにしても，モジュラ距離に関して三角不等式が成立することは明らかである．

式(6.1)で表される範囲の整数Ｎに対して負巡回けた移動が以下のように定義される．

［定義６．１］　hけたのST表現で表される整数を

$$N = (a_{h-1}a_{h-2}\cdots a_0)_{ST}$$

とする．このとき，整数

$$N' = (a_{h-2}\cdots a_0\bar{a}_{h-1})_{ST}$$

をＮの負巡回けた移動という．

hけたのST表現で表される任意の整数Ｎを同じ方向にh回負巡回けた移動することにより，整数-Ｎが得られる．これをさらにh回負巡回けた移動することにより再び，Ｎが得られるから，(2h-1)回負巡回けた移動することにより 2h個の整数が得られる．これらは，絶対値の等しい正と負の整数のh対である．負巡回けた移動の考え方を図６．２に示す．Ｎの負巡回けた移動Ｎ'は，

$$\begin{aligned} N' &= a_{h-2}3^{h-1} + \cdots + a_0 3 + \bar{a}_{h-1} \\ &= 3N - a_{h-1}(3^h+1) \end{aligned} \qquad (6.2)$$

であるから，Ｎ'は，３Ｎの法3^h+1に関する絶対最小剰余であり，

$$N' = 3N \bmod (3^h+1) \qquad (6.3)$$

と表すことができる．

［定義６．２］　ＳＴ－ＡＮ符号が負巡回けた移動のもとに閉じているとき，この符号を負巡回ＳＴ－ＡＮ符号という．

法3^h+1に関する絶対最小完全剰余系

$$Z_{A\cdot B} = \{0, \pm 1, \pm 2, \cdots, \pm(3^h-1)/2, (3^h+1)/2\}$$

を考える．この$Z_{A\cdot B}$は，法3^h+1に関して加算と乗算のもとに環を成す．3^h+1 を整除する任意の正整数をA'として，$Z_{A\cdot B}$におけるすべてのA'の倍数からなる部分集合 $I_{A\cdot}$に着目する．このとき，$I_{A\cdot}$ は，整数の環$Z_{A\cdot B}$においてA'で生成されるイディアルを成す．

$Z_{A\cdot B}$の元$(3^h+1)/2=(1\bar{1}\bar{1}\cdots\bar{1})_{ST}$ は，ST表現(h+1)けたを必要とするため，ST表現hけた上で負巡回けた移動を定義できないが，$Z_{A\cdot B}$から 元$(3^h+1)/2$を除いた集合を$Z_{\bar{A}\cdot B}$とすれば，$Z_{\bar{A}\cdot B}$の任意の元に対して負巡回けた移動を定義できる．$(3^h+1)/2$がイディアル $I_{A\cdot}$の元でなければ，定義６．２により，$I_{A\cdot}$は，負巡回けた移動のもとに閉じており，負巡回ＳＴ－ＡＮ符号である．他方，$(3^h+1)/2$ が $I_{A\cdot}$の元であれば，$I_{A\cdot}$から1個の元$(3^h+1)/2$を除いた集合は負巡回けた移動のもとに閉じており，このような集合もまた負巡回ＳＴ－ＡＮ符号である．　後者の場合，イディアル $I_{A\cdot}$は負巡回ＳＴ－ＡＮ符号そのものではないが，このような負巡回ＳＴ－ＡＮ符号もイディアル $I_{A\cdot}$に準じるものとして，便宜上，$I_{A\cdot}$で表すことにする．

負巡回ＳＴ－ＡＮ符号 $I_{A\cdot}$ の任意の符号語$A'N=(a_{h-1}a_{h-2}\cdots a_0)_{ST}$とするとき，A'Nの1けた左負巡回けた移動は，式(6.2)により，

$$(a_{h-2}\cdots a_0\bar{a}_{h-1})_{ST} = A'N \times 3 - a_{h-1}(3^h+1)$$

である．これは$Z_{\bar{A}\cdot B}$の元であり，A'の倍数であるから，$I_{A\cdot}$の元である．

負巡回ＳＴ－ＡＮ符号 $I_{A\cdot}$の生成数をA'，符号長をhとすれば，

$$A'B = 3^h+1 \qquad (6.4)$$

なる整数Bが存在して，このとき，(3,B)=1である．情報整数Nは法Bに関する絶対最小完全剰余系Z_Bの元である．ただし，$B/2 \in Z_B$ なら，B/2を除くものとする．

このような集合をZ_Bで表す．負巡回ＳＴ－ＡＮ符号 $I_{A'}$ は $\bar{Z}_B$ の元のA'倍からなる集合であり，$I_{A'}$ は

$$I_{A'} = A' \cdot \{e \mid e \in Z_B,\ e \neq B/2\}$$

$$= A' \cdot \{e \mid e \in \bar{Z}_B\} \qquad (6.5)$$

のように表せる．ここに，Bが奇数なら，B/2はZ_Bの元でなく，Bは符号語数を表す．また，Bが偶数なら，B/2はZ_Bの元であり，$\bar{Z}_B$はこれを除いたものであるから，B-1 が符号語数を表す．

このような負巡回ＳＴ－ＡＮ符号 $I_{A'}$ の分解は，巡回ＳＴ－ＡＮ符号 I_A の分解（第４章２節参照）とほとんど類似しており，同様の議論の展開が可能である．

$I_{A'}$ は，巡回ＳＴ－ＡＮ符号と同様，Bの約数d_jにより，いくつかの部分符号 $A'd_j \cdot G(B/d_j)$ に分解される．ただし，$A'B/2 \cdot G(2) = A'B/2$ は含まないものとする．さらに，これらの部分符号は，$G(B/d_j)$ の巡回部分群 $H_{(1)}(B/d_j)$ によるコセット展開を利用して，$\nu_j = \varphi(B/d_j)/E(3,B/d_j)$ 個の素符号 $A'd_j \cdot H_{(p)}(B/d_j)$ に分解される．このとき，各素符号は，そこに含まれる符号語の任意のひとつを負巡回けた移動したもので尽くされる．また，$I_{A'}$ の{0}以外の素符号に対応するコセットにおいて，$\bar{Z}_B$の元eと-eは必ず同一のコセットに属する．すなわち，$I_{A'}$ の符号語 A'N と -A'N は同じ素符号に属する．

例６．１　生成数A'=193とすると，$193 \times 34 = 3^8+1$（第３章表３．４参照）により，ＳＴ－ＡＮ符号の符号長hと整数Bが，

$h=8,\ B=(3^8+1)/193=34$

で与えられる．この負巡回ＳＴ－ＡＮ符号 $I_{A'}$ は

$$I_{A'} = 193 \cdot G(34) + 386 \cdot G(17) + 6562 \cdot G(1),$$

$$G(1) = \{0\},$$

$$G(17) = \{\pm1, \pm2, \pm3, \pm4, \pm5, \pm6, \pm7, \pm8\},$$

$$G(34) = \{\pm1, \pm3, \pm5, \pm7, \pm9, \pm11, \pm13, \pm15\}$$

のように，3個の部分符号に展開される．このとき，$3281 \cdot G(2) = (3^8+1)/2$ は含ま

れない．6562・G(1)は1個の符号語からなり，

$6562\cdot G(1)=(00000000)_{ST}$

である．386・G(17)と193・G(34)は，$\varphi(17)=E(3,17)=16$, $\varphi(34)=E(3,34)=16$であるから，共に1個の部分群からなり，

$G(17)=H_{(1)}(17)$，$G(34)=H_{(1)}(34)$

である．たとえば，素符号$193\cdot H_{(1)}(34)$に含まれる $l_{A'}$ の符号語は，

$193 = (001\bar{1}1011)_{ST}$　　$-193 = (00\bar{1}1\bar{1}0\bar{1}\bar{1})_{ST}$

$579 = (01\bar{1}10110)_{ST}$　　$-579 = (0\bar{1}1\bar{1}0\bar{1}\bar{1}0)_{ST}$

$1737 = (1\bar{1}101100)_{ST}$　　$-1737 = (\bar{1}1\bar{1}0\bar{1}\bar{1}00)_{ST}$

$-1351 = (\bar{1}1011001)_{ST}$　　$1351 = (1\bar{1}0\bar{1}\bar{1}001)_{ST}$

$2509 = (10110011)_{ST}$　　$-2509 = (\bar{1}0\bar{1}\bar{1}0011)_{ST}$

$965 = (01100\bar{1}1\bar{1})_{ST}$　　$-965 = (0\bar{1}\bar{1}001\bar{1}1)_{ST}$

$2895 = (1100\bar{1}1\bar{1}0)_{ST}$　　$-2895 = (\bar{1}\bar{1}001\bar{1}10)_{ST}$

$2123 = (100\bar{1}1\bar{1}0\bar{1})_{ST}$　　$-2123 = (\bar{1}001\bar{1}101)_{ST}$

であり，これら16個の符号語は任意のひとつを負巡回けた移動したもので尽くされる．

負巡回ＳＴ－ＡＮ符号 $l_{A'}$ に対して，法3^h+1に関するモジュラST距離（第２章参照）を導入する．この符号の最小重みと最小距離はこのモジュラ重み，モジュラ距離によって，巡回ＳＴ－ＡＮ符号 l_A の場合と同様に定義される．さらに，最小距離と誤り訂正能力の関係についても，モジュラ距離の性質２．９～２．11により，巡回ＳＴ－ＡＮ符号の場合（定理４．２，系４．１）と全く同様な以下の定理と系が成立する．

［定理６．１］　最小距離d_mが d+1 以上のとき，そのときに限って，d重以下のすべての算術誤りの検出が可能である．また，d_mが 2t+1 以上であるとき，そのときに限って，t重以下のすべての算術誤りの訂正が可能である．

（証明）　（定理４．２参照）

［系６．１］　最小距離d_mが t+d+1 以上のとき，t重以下のすべての算術誤りを訂正し，d(>t)重以下のすべての算術誤りを検出することが可能である．（証明略）

６．３　巡回ＳＴ－ＡＮ符号との関係

3と互いに素な正整数をBとするとき，

$$3^g+1 \equiv 0 \pmod{B}$$

を満たす最小の正整数 g が存在するなら，このようなgをG(3,B)で表す．このとき，符号長と生成数が

$$h = G(3,B),\quad A' = \frac{3^h+1}{B} \qquad (6.6)$$

で与えられるＳＴ－ＡＮ符号は負巡回ＳＴ－ＡＮ符号 $I_{A'}$ である．G(3,B)は任意の整数Bに対して常に存在するというわけではない(第３章，表３．１の G(3,A) 参照)が，以下では，このようなBによって規定される負巡回ＳＴ－ＡＮ符号 $I_{A'}$ を考える．

ある整数Bで規定される負巡回ＳＴ－ＡＮ符号 $I_{A'}$ の符号長hと法Bに関して3が属するべき数E(3,B)との間には，

$$h = G(3,B) = E(3,B)/2 \qquad (6.7)$$

が成立する．前章で述べたように，E(3,B)はBで規定される巡回ＳＴ－ＡＮ符号の符号長nである．Bで規定される負巡回ＳＴ－ＡＮ符号が存在するなら，同じBで規定される巡回ＳＴ－ＡＮ符号が必ず存在して，その符号長は，n＝2hである．このとき，

$$AB = 3^n-1 = (3^h+1)(3^h-1)$$
$$= A'B(3^h-1)$$

であるから，両符号 I_A ， $I_{A'}$ の生成数の間には，

$$A = A'(3^h-1)$$

が成立する．したがって，Z_B^-の任意の元Nに対して，

$$AN = A'N(3^h-1) = (A'N)3^h + (-A'N)$$

であり，巡回ＳＴ－ＡＮ符号 I_A の符号語ANの上位hけたは負巡回ＳＴ－ＡＮ符号 $I_{A'}$の符号語A'Nであり，下位のhけたは $I_{A'}$の符号語-A'Nである．しかも，これらは同じ素符号に属する．

例６．２　先の例６．１の負巡回ＳＴ－ＡＮ符号に対応する巡回ＳＴ－ＡＮ符号は，符号語数B=34，符号長n=E(3,34)=16，生成数A=$(3^{16}-1)/34$=1266080 であり，

$$I_A = 1266080\cdot G(34) + 2532160\cdot G(17) + 21523360\cdot G(2) + 43046720\cdot G(1)$$

のように，4個の部分符号からなる．部分符号1266080・G(34)は強巡回的な素符号であり，この符号語1266080と対応する $I_{A'}$の素符号193・G(17)の符号語は，それぞれ，

$$1266080 = (00\bar{1}\bar{1}011\ 00\bar{1}\bar{1}\bar{1}0\bar{1}\bar{1})_{ST},$$

$$193 = (00\bar{1}\bar{1}011)_{ST},\ -193=(00\bar{1}\bar{1}\bar{1}0\bar{1}\bar{1})_{ST}$$

である．実際，I_A の符号語の上位8けたは負巡回ＳＴ－ＡＮ符号 $I_{A'}$の符号語 193 が，下位の8けたは $I_{A'}$の符号語 -193 がそれぞれ対応している．

3と互いに素な任意の整数Bに対して，G(3,B)が常に存在するとは限らないが，Bの約数d_j(ただし，BとB/2を除く)のすべてに対応する部分群G(B/d_j)に含まれるすべてのコセット$H_{(d)}$(B/d_j)において，

$$e \in H_{(d)}(B/d_j) \longleftrightarrow -e \in H_{(d)}(B/d_j)$$

を満たすとき，このようなBで規定される負巡回ＳＴ－ＡＮ符号が必ず存在する．

６．４　負巡回ＳＴ－ＡＮ符号の最小距離

巡回ＳＴ－ＡＮ符号の{0}以外のすべての部分符号がそれぞれ１個の素符号からなっているとき，各素符号には絶対値の等しい正と負の符号語の対が必ず含まれ

ており，対応するコセットについても，eと-eの対が同じコセットに属している．したがって．このような場合，同じBで規定される負巡回ＳＴ－ＡＮ符号が存在する．前章で述べた巡回ＳＴ－ＡＮ符号のうち，このようなものは，(a),(b),(d),(e)の４つの型である．それぞれに対応する負巡回ＳＴ－ＡＮ符号の最小距離の算定に関して，以下の定理群が成立する．ただし，pは5以上の素数とする．

(a)　B=p，2p

［定理６．２］　法pに関して3が原始根のとき，B=pで規定される符号 $l_{A'}$ の符号長と生成数は，

$$h = (p-1)/2,\quad A' = (3^h+1)/p \tag{6.8}$$

であり，その最小距離は，

$$d_m = \begin{cases} (p-1)/3, & (p \equiv 1 (\mathrm{mod}\ 3)) \\ (p+1)/3, & (p \equiv -1 (\mathrm{mod}\ 3)) \end{cases} \tag{6.9}$$

である．　（証明略）

［定理６．３］　法pに関して3が原始根のとき，B=2pで規定される符号 $l_{A'}$ の符号長と生成数は，

$$h = (p-1)/2,\quad A' = (3^h+1)/(2p) \tag{6.10}$$

であり，その最小距離は，

$$d_m = \begin{cases} (p-1)/3, & (p \equiv 1 (\mathrm{mod}\ 3)) \\ (p-2)/3, & (p \equiv -1 (\mathrm{mod}\ 3)) \end{cases} \tag{6.11}$$

である．　（証明略）

(b)　$B=p^{\alpha}$，$2p^{\alpha}$（αは2以上の整数）

［定理６．４］　法p^{α}に関して3が原始根のとき，$B=p^{\alpha}$で規定される符号 $l_{A'}$ の符号長と生成数は，

$$h = p^{\alpha}(p-1)/2,\quad A' = (3^h+1)/p^{\alpha} \tag{6.12}$$

であり，その最小距離は，

$$d_m = \begin{cases} (p^{\alpha} - p^{\alpha-1})/3, & (p \equiv 1 \pmod 3) \\ (p^{\alpha} - p^{\alpha-1} - 2p^{\alpha-2})/3, & (p \equiv -1 \pmod 3) \end{cases} \qquad (6.13)$$

である．　（証明略）

［定理６．５］ 法p^{α}に関して3が原始根のとき，$B=2p^{\alpha}$で規定される符号 I_{α} の符号長と生成数は，

$$h = p^{\alpha}(p-1)/2, \quad A' = (3^h+1)/(2p^{\alpha}) \qquad (6.14)$$

であり，その最小距離は，

$$d_m = \begin{cases} (p^{\alpha} - p^{\alpha-1})/3, & (p \equiv 1 \pmod 3) \\ (p^{\alpha} - 2p^{\alpha-1})/3, & (p \equiv -1 \pmod 3) \end{cases} \qquad (6.15)$$

である．　（証明略）

これらの符号の誤り訂正能力は符号長hに対する最小距離(d_m/h)の値が約2/3であり，定理６．２，６．３の場合は事実上の限界値となっており，対応する巡回ＳＴ－ＡＮ符号の場合と同じ値をもつ．これら以外のBで規定される負巡回ＳＴ－ＡＮ符号の最小距離は，巡回ＳＴ－ＡＮ符号の場合と同様，電子計算機を用いて５章２節の算定手順に基づいて組織的に算定することができる．

６．５　結　言

負巡回ＳＴ－ＡＮ符号は，任意の符号語数Bに対して存在するわけではないが，Bで規定される負巡回ＳＴ－ＡＮ符号が存在するなら，同じBで規定される巡回ＳＴ－ＡＮ符号が必ず存在する．このような符号と対応する負巡回ＳＴ－ＡＮ符号の符号長と生成数および符号語の関係を示した．とくに，Bの約数に基づく符号の分解においては，G(2)を除いて，同じ$G(B/d_j)$が対応し，個々に対応する符号語が存在する．このような巡回ＳＴ－ＡＮ符号の結果の多くを負巡回ＳＴ－ＡＮ符

号に応用することができる．このため，誤り訂正能力の大きな符号を容易に構成することができる．また，ST表現に基づく法3^n+1に関する加減算や負巡回けた移動の操作は，減算や負数の表現に補数を用いる2進の場合に比べて単純であり，負巡回ＳＴ－ＡＮ符号は，２進の負巡回ＡＮ符号[18]より実際的であると考えられる．

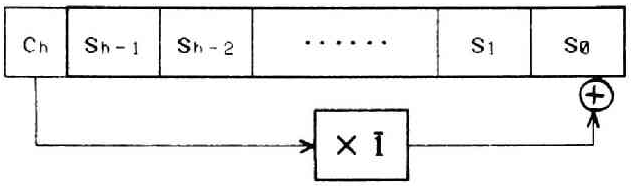

図６．１　法3^h+1に関する加算に伴う負循環けた上げ

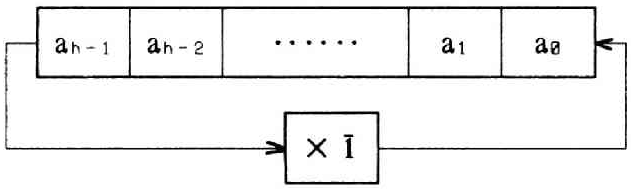

図６．２　ST表現hけた上の負巡回けた移動

第７章　ＳＴ－ＡＮ符号の復号

７．１　緒　言

本章では，３章から６章までに述べたＳＴ－ＡＮ符号の復号を提案する．はじめに，一般的なＳＴ－ＡＮ符号の誤り訂正の原理と復号方法について述べる．次ぎに，巡回ＳＴ－ＡＮ符号の誤り訂正の原理とこれに基づくエラー・トラッピング復号を提案する．代数的巡回符号の復号方法として開発されている窓付きエラー・トラッピング復号[20]を巡回ＳＴ－ＡＮ符号の場合に拡張する．その復号手順を提案する．さらに，個々の巡回ＳＴ－ＡＮ符号に対して，これらの復号手順が有効であるかどうかを調査する簡便な一方法を示し，窓付きエラー・トラッピング復号が有効な符号の例を求める．また，６章で述べた負巡回ＳＴ－ＡＮ符号の復号方法についても，巡回ＳＴ－ＡＮ符号の場合に準じてこれらの復号手順が適用できることを示す．最後に，多数決論理復号可能な巡回ＳＴ－ＡＮ符号のいくつかのクラスについて述べ，それらの復号手順を示す．

７．２　ＳＴ－ＡＮ符号の一般的な復号

ここで取り扱う算術誤りEの範囲を

$$-AM_{ST}(A,d)/2 < E < AM_{ST}(A,d)/2$$

とする．符号語ANに算術誤りEが生じて受信語V=AN+Eを得たとする．このとき，ANからVまでのST算術距離は，$D_{ST}(AN,V)=W_{ST}(E)$で与えられる．

算術誤りは，受信語がどの符号語にも一致しないことにより検出され，また，受信語が最も近い距離にある符号語に復号することにより訂正される．ＳＴ－ＡＮ符号の最小距離（ST算術距離に基づく）と誤り訂正能力の間には，定理３．３，３．４および系３．１が成立する．

［定義７．１］　受信語Vの法Aに関する絶対最小剰余をVのシンドロームといい，S(V)で表す．

シンドロームS(V)は，

$$S(V) = V \bmod A$$
$$= (AN+E) \bmod A$$
$$= E \bmod A$$

であるから，符号語ANには関係せず，算術誤りEのみによって定まる．

［定理７．１］　検出可能なd重以下の算術誤りE（≠0）のシンドロームは0でない．

（証明）　d重以下の算術誤りEはその定義により，$0 < W_{ST}(E) \leqq d$であるから，Eは符号語ではありえず，AはEを整除しない．　（証明終）

定理３．４に基づく訂正可能なt重以下の算術誤りを正当な誤りという．

［定理７．２］　正当なt重以下の誤りEとそのシンドロームは一対一に対応する．

（証明）　相異なる正当な誤りE_1，E_2のシンドロームが等しく，$S(E_1)=S(E_2)$とする．このとき，E_1-E_2はAの倍数であるから，$W_{ST}(E_1-E_2)>2t$である．他方，E_1，E_2のST算術重みは共にt以下であるから，

$$W_{ST}(E_1-E_2) \leqq W_{ST}(E_1)+W_{ST}(E_2) \leqq 2t$$

なる矛盾を生じる．それゆえ，$S(E_1)\neq S(E_2)$である．　（証明終）

上の定理によれば，t重以下のすべての正当な誤りとそのシンドロームとの対応表を用いて，これらの正当な誤りを訂正することができる．このとき，

$$S(-E) = -S(E)$$

であるから，その表を半減することができる．

例として，A=193で生成されるＳＴ－ＡＮ符号を考える．表３．４により，M_{ST}(193,5)=34であるから，情報整数の範囲を-17＜N＜17に限れば，この符号の最小距離はd_m=5であり，-3281＜E＜3281なる範囲の2重以下の算術誤りはすべて正当な誤りである．これらの正当な誤りとシンドロームを表７．１に示す．

［系７．１］ E_1を正当なt重以下の誤りとして，

$$E_1 = q_1A+S(E_1)$$

と表すことができる．また，E_2を

$$E_2 = q_2A+S(E_1),\quad (-M_{ST}(A,2t+1)/2<q_2<M_{ST}(A,2t+1)/2)$$

とする．$q_2=q_1$のとき，そのときに限って，$W_{ST}(E_2)\leqq t$である．

（証明）　$q_2=q_1$とすれば，明らかに $E_2=E_1$であり，$W_{ST}(E_2)=W_{ST}(E_1)\leqq t$である．$q_2\neq q_1$であって，$W_{ST}(E_2)\leqq t$とする．このとき，$E_2$は正当な誤りであって，$S(E_2)=S(E_1)$である．これは，定理７．２に矛盾する．　（証明終）

正当なt重以下の誤りEが符号語ANに生じて受信語V=AN+Eを得たとする．受信語Vのシンドローム$S(V)$は，VをAで割って，その絶対最小剰余をとることにより求めることができる．この$S(V)$に順次，

$$qA,\ (q=0,\pm1,\pm2,\cdots,\pm(M_{ST}(A,2t+1)-2)/2)$$

を加算して，各$qA+S(V)$のST算術重みを求め，その値がt以下になれば，そのような$qA+S(V)$が実際に発生した算術誤りEである．

先の例で示したA=193で生成される2重誤り訂正ＳＴ－ＡＮ符号の場合を考える．正当な誤りE=648=$(010\bar{1}0000)_{ST}$が符号語AN=386に生じて，受信語V=1034を得たとする．このとき，$S(V)$は69=$(10\bar{1}\bar{1}0)_{ST}$であり，$W_{ST}(S(V))>2$であるから，$S(V)$自身が正当な誤りではない．順次，以下のように$qA+S(V)$を求める．

$$A + S(V) = 262 = (101\bar{1}01)_{ST},\quad -A + S(V) = -124 = (\bar{1}11111)_{ST},$$

$$2A + S(V) = 455 = (1\bar{1}01\bar{0}1\bar{1})_{ST},\quad -2A + S(V) = -317 = (\bar{1}\bar{1}01\bar{1}1)_{ST},$$

$$3A + S(V) = 648 = (10\bar{1}0000)_{ST}$$

q=3 のとき，そのST算術重み$W_{ST}(3A+S(V))$が2以下となる．このため，実際に生じた算術誤りは E＝3A+S(V)＝648 であり，受信語V=1034からE=648を引算することにより，符号語AN=386を復元できる．

７．３　巡回ＳＴ－ＡＮ符号の復号

ここで取り扱う算術誤りEは，雑音や装置の障害のため，符号語ANに算術的に加えられるST表現nけた以下の正負の整数である．受信語をVとすれば，V=AN+Eで与えられる．このとき，ANからVまでのモジュラST距離は，

$$D_{MST}(AN,V) = W_{MST}(E) = W_{ST}(E)$$

で与えられる．巡回ＳＴ－ＡＮ符号の最小距離（法3^n-1に関するモジュラST距離に基づく）と誤り訂正能力の間には，定理４．２．および系４．１が成立する．これらの定理と系に基づく訂正可能な算術誤りを正当な誤りという．巡回ＳＴ－ＡＮ符号においても，一般のＳＴ－ＡＮ符号と同様，正当な誤り E とそのシンドローム S(E)に対して，定理７．１，７．２が成立する．

巡回ＳＴ－ＡＮ符号の任意の符号語ANを巡回けた移動したものはまた符号語であって，Aの倍数である．正当な誤りEの巡回けた移動は同じ算術重みをもつ正当な誤りてある．Eおよびその巡回けた移動（合計n個）の正当な誤りを巡回的に等価な誤りという．正当な誤りEおよび巡回的に等価な誤りのうち，絶対値が最小のものE_mをEの絶対最小巡回シフトという．

すべての正当な誤りからこのような E_m を抜き出し，これらのシンドローム$S(E_m)$との対応表と巡回けた移動を利用して，誤りの訂正が可能である[12]．この方法は，前節に述べたE－S(E)対応表のみによる方法に比べて，その対応表を小さくできる．

７．３．１　エラー・トラッピング復号

［定理７．３］　正当なt重誤りEが法Aに関する絶対最小完全剰余系Z_Aに属さないなら，EのシンドロームS(E)の算術重み$W_{ST}(S(E))$は t+1 以上である．

（証明）　正当なt重誤りEのシンドロームをS(E)とすると，EがZ$_n$の元でないとき，

$$E = AQ + S(E),\ (Q \neq 0)$$

なる整数商Qが存在する．AQ＝E－S(E) は，0以外の符号語であり，その算術重みは，定理４．２により，2t+1以上である．また，Eの算術重みがt以下であるから，

$$2t+1 \leqq W_{ST}(E-S(E)) \leqq W_{ST}(E) + W_{ST}(S(E)) \leqq t + W_{ST}(S(E))$$

である．したがって，$t+1 \leqq W_{ST}(S(E))$ である．　（証明終）

［系７．２］　d重誤り検出t重誤り訂正符号(d>t)において，$t+1 \leqq W_{ST}(E) \leqq d$なる算術誤りEのシンドロームS(E)の算術重み$W_{ST}(S(E))$は t+1 以上である．

（証明）　このような算術誤りEがZ$_n$の元なら，S(E)＝Eであり，明らかに，$t+1 \leqq W_{ST}(E) = W_{ST}(S(E))$である．EがZ$_n$の元でないなら，

$$E = AQ + S(E),\ (Q \neq 0)$$

なる商Qが存在し，AQ＝E－S(E)は0以外の符号語である．したがって，その算術重みは，系４．１により，d+t+1以上である．また，$W_{ST}(E) \leqq d$ であるから，

$$d+t+1 \leqq W_{ST}(E-S(E)) \leqq W_{ST}(E) + W_{ST}(S(E)) \leqq d + W_{ST}(S(E))$$

であり，$t+1 \leqq W_{ST}(S(E))$である．　（証明終）

正当なt重以下の算術誤りEがZ$_n$に属するなら，E＝S(E)であって，その算術重みはt以下である．逆に，次の系が成立する．

［系７．３］ 正当なt重以下の誤りEを生じた受信語V=AN+Eのシンドローム$S(V)$に対して，$W_{ST}(S(V)) \leqq t$ なら，

$$E = S(V) \qquad (7.1)$$

である．

（証明）　正当な誤りEがS(V)に等しくないと仮定すると，EはZ₀の元ではない．このとき，定理７．３，系７．２により，t+1≦W_{ST}(S(E))である．これは仮定に反する．　（証明終）

正当な誤りEの絶対最小巡回シフトE_mのすべてがZ_0に属するとは限らないが．E_mのすべてがZ_0に属する巡回ＳＴ－ＡＮ符号も存在する．たとえば，１重誤りの絶対最小巡回シフトE_mは±1のいずれかであり，Z_0の元である．また，ここでは．E_mのすべてがZ_0に属する２重誤り訂正符号の場合を示す．

例７．１　n=12，A=7592=$(101111\bar{1}\bar{1}\bar{1})_{ST}$，B=70 の巡回ＳＴ－ＡＮ符号は，最小距離が$d_m$=6であり（第５章参照），2重誤りの訂正と3重誤りの検出が可能(t=2,d=3)である．正当な誤りの絶対最小巡回シフトのうち，最大のものをE_{mx}で表すことにする．E_{mx}=$(000001000001)_{ST}$=730 は A/2未満であるから，E_{mx}はZ_0の元である．それゆえ，1重誤りと2重誤りの絶対最小巡回シフトE_mのすべてがZ_0の元である．

このような巡回ＳＴ－ＡＮ符号においては，定理７．３，系７．３に基づく次の復号手順が適用できる．

《復号手順７．１》

Ⅰ．受信語V=V_0のシンドロームS(V_0)＝0なら，誤りなしとして，Ⅴ．へ，
S(V_0)≠0なら，Ⅱ．へ．

Ⅱ．V_0またはその i 回左巡回けた移動V_iのシンドロームS(V_i)，(0≦i＜n)の算術重みがW_{ST}(S(V_i))≦tなら，V_i－S(V_i)を計算して，これをi回逆巡回けた移動した後，Ⅴ．へ，
W_{ST}(S(V_i))＞tなら，Ⅲ．へ．

Ⅲ．V_iを１けた左巡回けた移動し，i=i+1として，i<nなら，Ⅱ．へ，
i=nなら，Ⅳへ．

Ⅳ．訂正不能な(t+1)重以上の誤りを検出．

Ｖ． 生成数Aで除算する．

以上の復号手順を単純エラー・トラッピング復号と呼ぶことにする．

例７．２　例７．１の巡回ＳＴ－ＡＮ符号において，符号語

$$AN = 7592 = (0001011\bar{1}1\bar{1}\bar{1}\bar{1})_{ST}$$

に，正当な2重誤り

$$E = 157464 = (10\bar{1}000000000)_{ST}$$

が加わって，受信語

$$V = 165056 = (10\bar{1}101\bar{1}1\bar{1}\bar{1}\bar{1})_{ST}$$

を得たとする．受信語およびその巡回けた移動V_iとそのシンドローム$S(V_i)$は以下のようになる．

$V_0 = 165056 = (10\bar{1}101\bar{1}1\bar{1}\bar{1}\bar{1})_{ST}$　　$S(V_0) = -1968 = (\bar{1}010\bar{1}010)_{ST}$

$V_1 = -36272 = (0\bar{1}101\bar{1}1\bar{1}\bar{1}\bar{1}1)_{ST}$　　$S(V_1) = 1688 = (1\bar{1}100\bar{1}\bar{1}\bar{1})_{ST}$

$V_2 = -108816 = (\bar{1}101\bar{1}1\bar{1}\bar{1}\bar{1}10)_{ST}$　　$S(V_2) = -2528 = (\bar{1}0\bar{1}\bar{1}\bar{1}101)_{ST}$

$V_3 = 204992 = (1011\bar{1}1\bar{1}\bar{1}10\bar{1})_{ST}$　　$S(V_3) = 8 = (00000\bar{1}0\bar{1})_{ST}$

この場合，3回左巡回けた移動した時点で，シンドローム$S(V_3)$の算術重みが2となる．したがって，$V_3 - S(V_3)$を計算して，これを3回逆巡回けた移動することにより，符号語ANを復元できる．

[定理７．４] 受信語またはそのi回左巡回けた移動V_i,(i=0,1,2,･･･,n-1)のシンドロームを$S(V_i)$とするとき，

$$S(V_i) = S(3S(V_{i-1})) \qquad (7.2)$$

である．　（証明略）

上の定理７．４により，先の単純エラー・トラッピング復号(復号手順７．１)を少し簡単にすることができる．すなわち，受信語V_0のシンドロームを求めるのに，

nけたの受信語を生成数で除算しなければならないが，受信語の左巡回けた移動V_iのシンドロームを求める際には，V_iよりもけた数の小さい$S(V_{i-1})$の3倍を生成数で除算し，その絶対最小剰余をとればいい．例７．２では，受信語のシンドローム

$$S(V_0) = -1968 = (\bar{1}010\bar{1}010)_{ST}$$

の3倍

$$3S(V_0) = -5904 = (\bar{1}010\bar{1}0100)_{ST}$$

をAで除算して，

$$S(V_1) = 3S(V_0) \bmod A = 1688$$

を得る．ここで，$3S(V_{i-1})$をAで割ってその絶対最小剰余を求める際，その時の商は 0 かまたは±1であるから，絶対最小剰余を求める操作もまた簡単となる．

７．３．２　窓付きエラー・トラッピング復号

巡回ＳＴ－ＡＮ符号によっては，復号手順７．１で示した単純エラー・トラッピングでは訂正できない正当な誤りが存在する場合がある．すなわち，正当な誤りEの絶対最小巡回シフトがZ_Aの元でなければ，定理７．３により，E_mと巡回的に等価な誤りのシンドロームがことごとく t+1 以上となり，系７．３に基づく単純エラー・トラッピングでこのような正当な誤りを訂正することは不可能である．以下，このような巡回ＳＴ－ＡＮ符号の復号を考える．

単純エラー・トラッピングで訂正できない誤りに対する絶対最小巡回シフトE_mとそのシンドローム$S(E_m)$の対応表を併用するエラー・トラッピング復号[12]が考えられる．その他の方法として，検査窓を用いるエラー・トラッピング復号がある．本節では，後者について述べるが，いずれにしても，まず，正当な誤りの絶対最小巡回シフトE_mのすべてがZ_Aに属するか否かについて調べる必要がある．

正当なｔ重誤りE_mのうち，最大のものをE_{mx}で表すことにする．このとき，$E_{mx} < A/2$なら，すべてのt重以下の正当な誤りの絶対最小巡回シフトはZ_Aに属し，このような誤りを単純エラー・トラッピングで訂正可能である．このため，tの種々の値に対して，E_{mx}を検討する．符号長が

$$n = qt + r, \quad (0 \leqq r < t) \qquad (7.3)$$

で表されるとき，E_{mx}は，q，t，r によって表７．２のように分類される．この表で．E_{mx}とそのパターン（E_{mx}のST表現）において，Xは q-1個の ”0” と 1個の ”1” の長さqの系列(00･･･01)を表すものとする．

例７．３　n=11，A=3851，B=46，d_m=7 の巡回ＳＴ－ＡＮ符号（第５章参照）は，定理４．３により，3重誤りの訂正が可能である．t=3とすると，式(7.3)により，q=3,r=2となる．表７．２から，

$$E_{mx} = (00010001001)_{ST} = 3^7+3^3+1 = 2215 > A/2$$

である．さらに，t=2とすると，q=5,r=1であるから，

$$E_{mx} = (00000100001)_{ST} = 3^5+1 = 244 < A/2$$

を得る．したがって，一部の3重誤りのみが単純エラー・トラッピングで訂正されない．3重誤りの絶対最小巡回シフトE_mのうち，$|E_m| > A/2$ を満たすものを調べる．ただし，E_mのパターンにおいて，同じ3けたに非零けたをもつものは2^3個存在するが，非零けたのすべてが ”1” のE_mのみを調べれば十分である．3重誤りの絶対最小巡回シフトのうち，Z_aに属さないE_mのすべてに誤り$\pm 3^7$がある．そのシンドローム$S(E_m)$との対応は以下のようになる．

E_m		$S(E_m)$	
$(000\bar{1}000\bar{1}00\bar{1})_{ST}$	=-2215	$(1\bar{1}1\bar{1}1\bar{1}1)_{ST}$	= 1636
$(000\bar{1}000\bar{1}001)_{ST}$	=-2213	$(1\bar{1}1\bar{1}1\bar{1}00)_{ST}$	= 1638
$(000\bar{1}0001001)_{ST}$	=-2161	$(1\bar{1}100\bar{1}\bar{1}1)_{ST}$	= 1690
$(000\bar{1}0001001)_{ST}$	=-2159	$(1\bar{1}100\bar{1}00)_{ST}$	= 1692
$(00010000\bar{1}00\bar{1})_{ST}$	= 2159	$(\bar{1}1\bar{1}00100)_{ST}$	=-1692
$(00010000\bar{1}001)_{ST}$	= 2161	$(\bar{1}1\bar{1}00111\bar{1})_{ST}$	=-1690
$(00010001001\bar{1})_{ST}$	= 2213	$(\bar{1}1\bar{1}1\bar{1}100)_{ST}$	=-1638
$(00010001001)_{ST}$	= 2215	$(\bar{1}1\bar{1}1\bar{1}111\bar{1})_{ST}$	=-1636

例７．３の符号において，Z_aに属さない絶対最小巡回シフトのすべてが 3^7のけ

たに誤り$\pm 3^7$がある．この3^7のけたを受信語およびその巡回けた移動から取り除いておけば，依然として残っている2重誤り$E_w=E_m \pm 3^7$は，A/2未満であり，単純エラー・トラッピングで訂正することが可能となる．

このようなけたを検査窓あるいは単に窓ということにする．検査窓が3^kのけた1カ所の場合の復号手順を以下に示す．

《復号手順７．２》

Ⅰ． 受信語V_0のシンドロームS(V_0)が0なら，誤りなしとして，Ⅴ.へ，S(V_0)≠0なら，Ⅱ.へ．

Ⅱ． V_0またはそのi回左巡回けた移動V_iのシンドロームS(V_i),(0≦i＜n)の算術重みが$W_{ST}(S(V_i)) \leqq t$なら，**復号手順７．１**（Ⅱ,Ⅲ）で誤りを訂正したのち，Ⅴへ．ただし，$W_{ST}(S(V_i)) > t,(i=0,1,\cdots,n-1)$なら，i=0としてⅢへ．

Ⅲ． $V'_i = V_i \pm 3^k$のシンドロームS(V'_i),(0≦i＜n) を計算する．これらのST重みが$W_{ST}(S(V_i)) \leqq t-1$なら，**復号手順７．１**（Ⅱ,Ⅲ）で誤りを訂正したのち，Ⅴへ．ただし，$W_{ST}(S(V'_i)) > t-1,(i=0,1,\cdots,n-1)$なら，Ⅳへ．

Ⅳ． 訂正不能な誤りを検出．

Ⅴ． 生成数Aで除算する．

以上のような復号手順を窓付きエラー・トラッピング復号と呼ぶことにする．

例７．１　例７．３の巡回ＳＴ－ＡＮ符号で，Z_μに属さないすべてのE_mが3^7のけたに最高位の非零をもつから，この位置に検査窓を設ける．これらのE_mの3^7のけたを0にすれば，結果として残される２重誤り$E_m \pm 3^7$はすべてZ_μに属するから，窓はこの位置１ヶ所で十分である．たとえば，符号語

$$AN = 3851 = (001\bar{1}\bar{1}10\bar{1}\bar{1}0\bar{1})_{ST}$$

に３重誤り

$$E = -19443 = (0\bar{1}000100\bar{0}\bar{1}0)_{ST}$$

を生じて，受信語

$V = -15592 = (0\bar{1}\bar{1}10\bar{1}0\bar{1}\bar{1}\bar{1}\bar{1})_{ST}$

が得られたとする．以下に，復号手順７．２に基づく V_i，V'_i，$S(V'_i)$をi=0から順に示す．

V_0：　$-15592 = (0\bar{1}\bar{1}10\bar{1}0\bar{1}\bar{1}\bar{1}\bar{1})_{ST}$

V'_0：$-13405 = (0\bar{1}100\bar{1}0\bar{1}\bar{1}\bar{1}\bar{1})_{ST}$，　$-17779 = (0\bar{1}010\bar{1}0\bar{1}\bar{1}\bar{1}\bar{1})_{ST}$

$S(V'_0)$;$-1852 = (\bar{1}0110111)_{ST}$，　$1764 = (1\bar{1}111\bar{1}00)_{ST}$

V_1：　$-46776 = (\bar{1}1\bar{1}0\bar{1}0\bar{1}\bar{1}\bar{1}\bar{1}0)_{ST}$

V'_1：$-44589 = (\bar{1}1\bar{1}1\bar{1}0\bar{1}\bar{1}\bar{1}\bar{1}0)_{ST}$，　$-48963 = (\bar{1}1\bar{1}\bar{1}\bar{1}0\bar{1}\bar{1}\bar{1}\bar{1}0)_{ST}$

$S(V'_1)$；$1623 = (1\bar{1}1\bar{1}0010)_{ST}$，　$1100 = (1\bar{1}\bar{1}\bar{1}\bar{1}\bar{1}\bar{1}\bar{1})_{ST}$

V_2；　$36818 = (1\bar{1}0\bar{1}0\bar{1}\bar{1}\bar{1}\bar{1}0\bar{1})_{ST}$

V'_2；　$39005 = (1\bar{1}000\bar{1}\bar{1}\bar{1}\bar{1}0\bar{1})_{ST}$，　$34631 = (1\bar{1}\bar{1}10\bar{1}\bar{1}\bar{1}\bar{1}0\bar{1})_{ST}$

$S(V'_2)$：　$495 = (01\bar{1}00100)_{ST}$，　$-28 = (0000\bar{1}00\bar{1})_{ST}$

この時点で，$W_{ST}(S(V'_2)) \leqq t-1=2$ となる．このため，

$$V'_2 - S(V'_2) = (36818 - 3^7) - (-28)$$
$$= 34659$$
$$= (1\bar{1}\bar{1}10\bar{1}\bar{1}0\bar{1}00)_{ST}$$

を２回逆巡回けた移動して，符号語ANに復元される．

上の復号手順７．２の$S(V'_i)$を求める際，

$$V'_i \bmod A = [V_i \bmod A \pm 3^k \bmod A] \bmod A$$

であるから，$V'_i = V_i \pm 3^k$の法Aに関する絶対最小剰余をとる代わりに，$\pm 3^k$のシンドロームをV_iのシンドロームに加算し，これの法Aに関する剰余を計算してもよい．例７．４の$S(V'_1)$において，$\pm 3^7 = \pm 2187$のシンドロームは，$S(\pm 3^7) = \mp 1664$であるから，

$S(V'_1) = [-564+(-1664)] \bmod 3851 = 1623$

を得る．以上のようなシンドローム間での計算は，単純エラー・トラッピングの場合と同様，対象となる数値のけた数をnより小さくできる．

７．３．３ 検査窓の配置

与えられた巡回ＳＴ－ＡＮ符号に対して，その符号長n，生成数A，誤り訂正能力tから，E_{mx}のパターン(表７．２)を利用して，以上述べたエラー・トラッピング復号（単純，または，窓付き）が有効かどうかを以下の順序で調査することができる．

(1) n，t，および表７．２からZ_Aに属さないt重以下の正当な誤りのE_{mx}を求める．このようなE_{mx}が存在しなければ，この巡回ＳＴ－ＡＮ符号の場合，単純エラー・トラッピング《復号手順７．１》で正当な誤りのすべてが訂正可能である．E_{mx}が存在すれば，次へ．

(2) Z_Aに属さない正当な誤りの絶対最小巡回シフト($E_{mx} \geqq |E_m| > A/2$)を生成する．ただし，E_mのうち，非零けたが”1”のもののみでよい．

(3) (2)で生成したE_mの最大値(正当なt重誤りのE_{mx})に対して，非零最高位のけたに窓を設ける．この窓によって訂正可能なE_mを取り除く．この結果，E_mが残っていなければ，この符号の場合，窓付きエラー・トラッピング《復号手順７．２》で正当な誤りのすべてが訂正可能である．E_mが残っているなら，このようなE_mを表示して終了することにする．

上の(3)の操作において，窓によりE_mが取り除かれるかどうかを調べる方法を以下の例で示す．

例７．５　符号長，生成数，符号語数，最小距離がそれぞれ，

n=20，A=12679216，B=275，d_m=12

の巡回ＳＴ－ＡＮ符号は５重誤りの訂正が可能である．したがって，t=5，4，3，･･･ に対して，E_{mx}のパターンは表７．２により得ることができ，(1)により，これらのE_{mx}を A/2と比較する．

$$A/2 = (0000011001\bar{1}101\bar{1}10\bar{1}10\bar{1})_{ST}$$

$$t=5;\ E_{mx} = (00010001000100010001)_{ST} > A/2$$
$$t=4;\ E_{mx} = (00001000010000100001)_{ST} > A/2$$

$$t=3;\ E_{mx} = (00000010000001000001)_{ST} < A/2$$

この結果，５重誤りと４重誤りの一部が単純エラー・トラッピングで訂正できないことがわかる．つぎの(2)の操作により，以下のような32個のE_mが生成される．

t=5; E_m = (00010001000100010001)$_{ST}$ ･･･ No.1 (= E_{mx})
(00001001000100010001)$_{ST}$ ･･･ No.2
(00001001000010010001)$_{ST}$ ･･･ No.3
(00001000100100010001)$_{ST}$ ･･･ No.4
(00001000100100001001)$_{ST}$ ･･･ No.5
(00001000100010010001)$_{ST}$ ･･･ No.6
(00001000100010001001)$_{ST}$ ･･･ No.7
(00001000100010000101)$_{ST}$ ･･･ No.8
(00001000100001010001)$_{ST}$ ･･･ No.9
(00001000100001001001)$_{ST}$ ･･･ No.10
(00001000100001000101)$_{ST}$ ･･･ No.11
(00001000011000010001)$_{ST}$ ･･･ No.12
(00001000010100010001)$_{ST}$ ･･･ No.13
(00001000010100001001)$_{ST}$ ･･･ No.14
(00001000010010010001)$_{ST}$ ･･･ No.15
(00001000010010001001)$_{ST}$ ･･･ No.16
(00001000010010000101)$_{ST}$ ･･･ No.17
(00001000010001010001)$_{ST}$ ･･･ No.18
(00001000010001001001)$_{ST}$ ･･･ No.19
(00001000010001000101)$_{ST}$ ･･･ No.20
(00001000010001000011)$_{ST}$ ･･･ No.21
(00001000010000110001)$_{ST}$ ･･･ No.22
(00001000010000101001)$_{ST}$ ･･･ No.23
(00001000010000100101)$_{ST}$ ･･･ No.24
(00001000010000100011)$_{ST}$ ･･･ No.25
(00000110010000100001)$_{ST}$ ･･･ No.26
(00000110001000100001)$_{ST}$ ･･･ No.27
(00000110001000010001)$_{ST}$ ･･･ No.28
(00000110000100100001)$_{ST}$ ･･･ No.29
(00000110000100010001)$_{ST}$ ･･･ No.30
(00000110000100001001)$_{ST}$ ･･･ No.31
t=4; E_m = (00001000010000100001)$_{ST}$ ･･･ No.32 (= E_{mx})

まず，窓は，これらEmの最大値，すなわち，t=5の場合のEm×の非零最高位のけた3^{16}に設ける．この窓により，取り除かれるEmを以下のようにして調べることができる．これはEmの非零けた "1" が3^{16}のけたに来るようEmを左へ巡回けた移動し，この "1" を除いた値Ew(=(Em×3^i) mod AB −3^{16}，0≦i<n)を求め，これとA/2との大小関係を比較する．このとき，EwがA/2未満なら，このEmを取り除く．この操作は最大t回(ただし，iはn-1まで)であり，この間でEwがA/2未満にならなければ，そのようなEmを残す．これらのEwを以下に示す（一部省略）．ここで，Ewの3^{16}のけた（窓）を"*"で示す．また，対応するEmの左巡回けた移動したものが，A/2以下になる i の値(最小値)を示す．

	A/2 = $(0000011001\bar{1}101\bar{1}10\bar{1}10\bar{1})_{ST}$		i
t=5;	$(000*0001000100010001)_{ST}$	… No.1	0
	$(000*0010001000100010)_{ST}$	… No.2	1
	$(000*0010000100100010)_{ST}$	… No.3	1
	$(000*0001001000100010)_{ST}$	… No.4	1
	・・・・・・・・・・・・・・・・・・		
	$(000*0001000010001010)_{ST}$	… No.11	1
	$(000*0000110000100010)_{ST}$	… No.12	1
	・・・・・・・・・・・・・・・・・・		
	$(000*0000100001000110)_{ST}$	… No.25	1
	$(000*0000100000110010)_{ST}$	… No.26	9
	$(000*0001000010000011)_{ST}$	… No.27	5
	$(000*0000100010000011)_{ST}$	… No.28	5
	$(000*0010000100000110)_{ST}$	… No.29	6
	$(000*0001000100000110)_{ST}$	… No.30	6
	$(000*0000100100000110)_{ST}$	… No.31	6
t=4;	$(000*0000100001000010)_{ST}$	… No.32	1

以上のEwはすべてA/2未満となり，このため，Emのすべてが取り除かれる．この結果，窓は3^{16}のけた１ヶ所で充分であることが判る．したがって，上の巡回ＳＴ－ＡＮ符号は，k＝16として，窓付きエラー・トラッピング**《復号手順７．２》**で正当な誤りのすべてが訂正可能である．

先に述べた(3)の操作の結果，E_mが残っていれば，E_mの最大値(正当なt重誤りのE_{mx})非零最高位のけた１個だけでなく，さらに２番目，３番目，･･･ に窓を設けなければ，このようなE_mを取り除くことができないことを意味する．このような場合，２番目以降の窓の位置を決定する簡便な一つの方法として，残っているE_mの最大値に対して，(3)の操作をE_mがなくなるまで繰り返し行う方法（図７．１）が考えられる．しかし，この方法は窓の個数最小を保障するものではない．

いずれにしても，このような窓により訂正される正当な誤りの個数があまり増えないにもかかわらず，復号手順７．２のⅢの繰り返し回数が多くなり，復号手順が複雑になる．このような場合，窓付きエラー・トラッピング復号(検査窓が２個以上)は実際的ではないが，最も簡単な検査窓が２個の場合の復号手順を示しておく．これは，検査窓が１個の場合の復号手順７．２のⅢにおいて，窓位置kを代えてこの操作Ⅲを２回繰り返すことにする．すなわち，復号手順７．２のⅢを以下のⅢ'に置き換えればよい．

《復号手順７．２'》

Ⅲ'．$V'_i = V_i \pm 3^{16}$のシンドロームS(V'$_i$),(0≦i＜n)を計算する．これらのST重みが$W_{ST}(S(V_i)) \leqq t-1$なら，**復号手順７．１**（Ⅱ，Ⅲ）で誤りを訂正したのち，Ⅴへ．ただし，$W_{ST}(S(V'_i)) > t-1$,(i=0,1,･･･,n-1)なら，$V''_i = V_i \pm 3^{14}$ のシンドロームS(V"$_i$),(0≦i＜n)に対して，上と同様の操作を行う．この操作(i=0,1,･･･,n-1)によってもその算術重み$W_{ST}(S(V''_i))$がt-1以下にならなければ，Ⅳへ．

先に述べた検査窓の配置を調査する手順(図７．１)に基づき，符号長の短い符号(n≦25)について計算機を用いて調査した．検査窓を必要とする符号の例を表７．３に示す．ここで，窓を２カ所以上必要とする符号は存在しなかった．また，同時に２個以上の窓(k_1,k_2,･･･)を設けて，受信語またはその巡回シフトV_iに対して，

$$V'_i = V_i \pm 3^{k_1} \pm 3^{k_2} \pm \cdots$$

のシンドロームを計算しなければならないような復号手順を要する符号もまたその符号長が25以下には存在しなかった．しかし，この場合にも復号の手数がさら

に増大し，窓の効果は一層減少すると考えられる．

７．４　負巡回ＳＴ－ＡＮ符号の復号

第６章で述べたように，ある整数Bで規定される負巡回ＳＴ－ＡＮ符号は同じBで規定される巡回ＳＴ－ＡＮ符号と構造的に深い関連をもつ．したがって，その復号方法に関してもまた同様であると考えられる．前に述べた巡回ＳＴ－ＡＮ符号の単純エラー・トラッピング復号に対応して，負巡回けた移動とそのシンドロームによる復号方法を提案する．

ここで取り扱う算術誤りEは，符号語A'Nに算術的に加えられるST表現hけた以下の正負の整数である．符号語A'Nから受信語Vまでのモジュラ ST距離は，

$$D_{MST}(AN,V) = W_{MST}(E) = W_{ST}(E)$$

で与えられる．負巡回ＳＴ－ＡＮ符号の最小距離（法3^h+1に関するモジュラST距離に基づく）と誤り訂正能力の間には，定理６．１，および系６．１が成立する．これらの定理と系に基づく訂正可能な算術誤りを正当な誤りという．負巡回ＳＴ－ＡＮ符号においても，一般のＳＴ－ＡＮ符号と同様，正当な誤りEとそのシンドロームS(E)に対して，定理７．１，７．２が成立する．

負巡回ＳＴ－ＡＮ符号の任意の符号語A'Nを負巡回けた移動したものはまた符号語であって，A'の倍数である．正当な誤りEの負巡回けた移動は同じ算術重みをもつ正当な誤りである．Eおよびその負巡回けた移動（合計2h個）の正当な誤りを負巡回的に等価な誤りという．正当な誤りEおよび負巡回的に等価な誤りのうち，絶対値が最小のものをE_mをEの絶対最小負巡回シフトという．

前節の巡回ＳＴ－ＡＮ符号のエラー・トラッピング復号に関する定理と系(定理７．３，系７．２，７．３)に対応して，以下の定理と系が成立する．法 3^h+1に関するモジュラST重みに対して三角不等式が成立する(第２章参照)から，これらの証明は，前節の定理等の証明と全く同様であるため，これらを省略する．

［定理７．５］　正当なt重誤りEが法A'に関する絶対最小完全剰余系$Z_{\cdot}$に属さないなら，EのシンドロームS(E)の算術重み$W_{ST}(S(E))$は t+1 以上である．

（証明略）

［系７．４］ d重誤り検出t重誤り訂正符号(d>t)において，$t+1 \leqq W_{ST}(E) \leqq d$なる算術誤りEのシンドロームS(E)の算術重み$W_{ST}(S(E))$は $t+1$ 以上である．

（証明略）

正当なt重以下の算術誤りEが$Z_{n,\cdot}$に属するなら，E＝S(E)であって，その算術重みはt以下である．逆に，次の系が成立する．

［系７．５］ 正当なt重以下の誤りEを生じた受信語V=A'N+EのシンドロームS(V)に対して，$W_{ST}(S(V)) \leqq t$ なら，

$$E = S(V) \tag{7.4}$$

である． （証明略）

以上の定理と系により，負巡回ＳＴ－ＡＮ符号に対しても，復号手順７．１に類似のエラー・トラッピング復号が有効である．以下の復号手順は，復号手順７．１の巡回けた移動を負巡回けた移動に，符号長 n を h に置き換えたものである．

《復号手順７．３》

Ⅰ． 受信語$V=V_0$のシンドロームS(V_0)＝0なら，誤りなしとして，Ⅴ．へ，
S(V_0)≠0なら，Ⅱ．へ．

Ⅱ． V_0またはそのi回負巡回けた移動V_iのシンドロームS(V_i),(0≦i＜h)の算術重みが$W_{ST}(S(V_i)) \leqq t$なら，$V_i - S(V_i)$を計算して，これをi回逆負巡回けた移動した後，Ⅴ．へ，
$W_{ST}(S(V_i)) > t+1$なら，Ⅲ．へ．

Ⅲ． V_iを１けた負巡回けた移動し，i=i+1として，i<h なら，Ⅱ．へ，
i=h なら，Ⅳへ．

Ⅳ． 訂正不能な(t+1)重以上の誤りを検出．

Ⅴ． 生成数A'で除算する．

例７．６　h=8，B=34，A'=193=$(001\bar{1}1011)_{ST}$ の負巡回ＳＴ－ＡＮ符号は，最小距離がd_m=5であり（第６章参照），2重誤りの訂正が可能(t=2)である．符号語

$$A' = 193 = (001\bar{1}1011)_{ST}$$

に2重誤り

$$E = 648 = (010\bar{1}0000)_{ST}$$

を生じて，受信語

$$V = 841 = (01011011)_{ST}$$

を得たとする．受信語およびその負巡回けた移動V_iとそのシンドロームS(V_i)は以下のようになる．

V_0= 841=$(01011011)_{ST}$　　S(V_0)= 69=$(10\bar{1}\bar{1}0)_{ST}$

V_1=2523=$(10110110)_{ST}$　　S(V_1)= 14=$(01\bar{1}\bar{1}\bar{1})_{ST}$

V_2=1007=$(01101101)_{ST}$　　S(V_2)= 42=$(1\bar{1}\bar{1}\bar{1}0)_{ST}$

V_3=3021=$(11011010)_{ST}$　　S(V_3)=-67=$(\bar{1}1\bar{1}\bar{1}\bar{1})_{ST}$

V_4=2501=$(10110\bar{1}0\bar{1})_{ST}$　　S(V_4)= -8=$(00\bar{1}01)_{ST}$

この場合，4回負巡回けた移動した時点で，シンドロームS(V_4)の算術重みが2となる．したがって，

$$V_4 - S(V_4) = 2501 - (-8)$$
$$= 2509$$
$$= (10110\bar{0}\bar{1}1)_{ST}$$

を4回逆負巡回けた移動することにより，符号語A'を復元できる．

以上の例からも明らかなように，巡回ＳＴ－ＡＮ符号のエラー・トラッピングに準じた負巡回けた移動とそのシンドロームによる誤り訂正が有効であり，巡回ＳＴ－ＡＮ符号の復号方法と同様の議論の展開が可能である．この負巡回ＳＴ－ＡＮ符号の場合にも，以下に例示するように検査窓による窓付きエラー・トラッピング復号が有効な符号が存在する．このとき，窓の最適配置の問題もまったく

同じ手順が適用できる．

例７．７　h=17，B=206，A'=626894 の負巡回ＳＴ－ＡＮ符号は，最小距離 d_m=12であり，４重誤りの訂正が可能である．したがって，t=4，3，･･･ に対して．E_{mx}のパターンは式(7.3)と表７．２により得ることができ，これらのE_{mx}を A'/2と比較する．

$$A'/2 = (0000\bar{1}\bar{1}\bar{1}10\bar{1}100\bar{1}011)_{ST}$$

$$t=4;\ E_{mx} = (0000100010001001)_{ST} > A'/2$$

$$t=3;\ E_{mx} = (0000010000010001)_{ST} < A'/2$$

これにより，一部の４重誤りのみが単純エラー・トラッピングで訂正できないことがわかる．これらのE_{mx}に基づき，$|E_{mx}| > A'/2$ を満たす非零けたが "1" のもののみを生成する．

$$\begin{aligned} t=4;\ E_m = {} & (0000100010001001)_{ST} \cdots \text{No.1 } (= E_{mx}) \\ & (0000100010000101)_{ST} \cdots \text{No.2} \\ & (0000100001001001)_{ST} \cdots \text{No.3} \\ & (0000100001000101)_{ST} \cdots \text{No.4} \\ & (0000100001000011)_{ST} \cdots \text{No.5} \end{aligned}$$

以上のE_mすべて3^{12}のけたに "1" をもつ．このため，窓を3^{12}のけたに設けることにより，正当な４重以下の誤りのすべてを訂正することができる．

上の例では，巡回ＳＴ－ＡＮ符号の窓付きエラー・トラッピング復号手順７．２の n を h(=17) に，巡回けた移動 を 負巡回けた移動 に置き換えた次の復号手順７．４(k=12として)が適用できる．

《復号手順７．４》

Ⅰ．受信語V_0のシンドロームS(V_0)が0なら，誤りなしとして，Ⅴ．へ，S(V_0)≠0なら，Ⅱ．へ．

Ⅱ．V_0またはそのi回負巡回けた移動V_iのシンドロームS(V_i)，(0≦i＜h)の算術重みがW_{ST}(S(V_i))≦tなら，**復号手順７．３**（Ⅱ，Ⅲ）で誤りを訂正したのち，Ⅴへ．ただし，W_{ST}(S(V_i))＞t，(i=0,1,･･･,h-1)なら，i=0としてⅢへ．

Ⅲ．$V'_i = V_i \pm 3^p$のシンドロームS(V'_i)，(0≦i＜h) を計算する．これらのST重

みが$W_{ST}(S(V_i))\leqq t-1$なら，復号手順７．３（Ⅱ,Ⅲ）で誤りを訂正したのち，Ⅴへ．ただし，$W_{ST}(S(V'_i))>t-1,(i=0,1,\cdots,h-1)$なら，Ⅳへ．

Ⅳ．訂正不能な誤りを検出．

Ⅴ．生成数A'で除算する．

７．５　多数決論理復号可能な巡回ＳＴ－ＡＮ符号の復号

符号語数Bに関するべき数の倍数でその符号長が定められる巡回ＳＴ－ＡＮ符号（第４章２節の繰り返し符号）は冗長度は大きいが，その最小距離は，第５章のような算定手順を必要とせず，生成数A あるいは 符号語数B の形から容易に定まる[40]．２進符号では，I.L.ErioshとS.L.Erosh[11]が，次に示すAの形の基本的なクラスを提案している．

$$A=\frac{2^{kd}-1}{2^k+1},\ A=\frac{2^{kd}+1}{2^k+1},\quad (d;\text{奇数})$$

$$A=\frac{2^{kd}-1}{2^k+1},\quad (d;\text{偶数})$$

この符号の基本的な概念を巡回ＳＴ－ＡＮ符号に拡張したものをＥＥ型巡回ＳＴ－ＡＮ符号という．

さらに，T.HwangとC.R.P.Hartmann[20]が提案したものは，以下のようなAの形のものである．

$$A=\frac{(2^{m_1}\pm1)(2^{m_2}\pm1)(2^n-1)}{(2^{n_1}\pm1)(2^{n_2}\pm1)},\quad (m_1,m_2,n_1,n_2;\text{正整数})$$

同様に，この符号を拡張したものをＨＨ型巡回ＳＴ－ＡＮ符号という．

また，Liuら[5]は，多数決論理復号可能な２進巡回ＡＮ符号とその復号方法を提案している．この復号方法はその手順の簡単さから重要な復号方法のひとつである．上のＥＥ型およびＨＨ型巡回ＳＴ－ＡＮ符号に対して，多数決論理復号が可能な代表的なものとその復号手順を示す．

７．５．１　１段多数決論理復号

符号長，生成数，および，その符号語数がそれぞれ，

$$n = n_1 n_2,\ A = (3^n-1)/(3^{n_1}-1),$$

$$B = 3^{n_1}-1,\ (n_1, n_2\ ;\text{正の奇数}) \qquad (7.5)$$

で与えられるＥＥ型巡回ＳＴ－ＡＮ符号を考える．この符号の任意の符号語ANは，

$$AN = (3^{n_1(n_2-1)} + 3^{n_1(n_2-2)} + \cdots + 3^{n_1} + 1)N \qquad (7.6)$$

のように表される．情報整数Nが法Bに関する絶対最小完全剰余系Z_Bの元であるから，

$$-(3^{n_1}-1)/2 < N \leqq (3^{n_1}-1)/2 \qquad (7.7)$$

であり，Nは n_1けた以下のST表現で表され，ANのST表現は，NのST表現をn_2回繰り返したものである．この符号の最小距離は $d_m=n_2$ である．

受信語をVとすれば，

$$V = (AN + E) \bmod A = (a_{n-1}a_{n-2}\cdots a_1 a_0)_{ST}$$

$$= N_{n_2-1}\times 3^{n_1(n_2-1)} + N_{n_2-2}\times 3^{n_1(n_2-2)} + \cdots$$

$$\cdots + N_1\times 3^{n_1} + N_0$$

のように表せる．ここに，N_i,(i=0,1,･･･,n_2-1)は VのST表現における$3^{n_1 i}$のけたから連続する上位n_1けたのST表現である．このようなNiを受信語Vの第iブロックという．

誤りがなくE=0のときは，当然，すべてのブロックがNに一致する．あるブロックに１重誤りE=±3^jが生じた場合を考える．

$-(3^{n_1}-1)/2<N<(3^{n_1}-1)/2$ のとき，符号語ANは連続するn_1けたの範囲に必ず"0"か，あるいは"1"（または"$\bar{1}$"）のけたがあり，１重誤りによるけた上がり（または けた借り）の伝搬はそのけたで止まる．このため，１重誤りによってこのような影響を受けるけた数はn_1けたを超えない．$N=(3^{n_1}-1)/2=(11\cdots1)_{ST}$のとき，符号語ANはnけたすべてが"1"となる．これに１重誤りE=3^jが生じると，

循環桁上げの操作により全けたにその影響をもたらし，その結果，受信語Vは3^jのけたが "0" になり，それ以外のけたはすべて "$\bar{1}$" となる．しかし，3^jのけたを含まないブロックに着目すれば，

$$-(3^{n_1}-1)/2 \equiv (3^{n_1}-1)/2 \pmod{B}$$

であるから，このようなブロックに対して，"$\bar{1}$" を "1" とみなすことができる．このようにすれば，1重誤りEの影響を受けるけたをその誤りを含むブロック(n_1けた)に納めることができる．以上のことから，次の定理が成立する．

[定理7.6] 受信語Vにおいて，

$$N_i = -(3^{n_1}-1)/2 = (\bar{1}\bar{1}\bar{1} \cdots \bar{1}\bar{1}\bar{1})_{ST}$$

なるブロックがあれば，これを

$$N_i' = (3^{n_1}-1)/2 = (111 \cdots 111)_{ST}$$

とする．このとき，すべての符号語ANに対して1重誤りによる影響は，n_1けたを超えない． （証明略）

受信語Vの各けたの記号を以下のようなn_1個の類，

$$C_0 = \{a_0, a_{n_1}, a_{2n_1}, \cdots, a_{(n_2-1)n_1}\},$$

$$C_1 = \{a_1, a_{n_1+1}, a_{2n_1+1}, \cdots, a_{(n_2-1)n_1+1}\},$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$C_j = \{a_j, a_{n_1+j}, a_{2n_1+j}, \cdots, a_{(n_2-1)n_1+j}\},$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$C_{n_1-1} = \{a_{n_1-1}, a_{2n_1-1}, \cdots, a_{n_2n_1-1}\}$$

に分ける．すなわち，この類C_jは，受信語Vの各ブロックN_iの第jけたの集合である．C_jにおいて隣接する2けたは，VのST表現において，n_1けただけ離れている．このため，定理7.6によれば，1重誤りによってC_jの2けた以上が影響を受けることはない．誤りを含まない受信語（符号語）の場合は，C_jの n_2個の要素はすべて等しい．

誤りEのST算術重みを

$W_{ST}(E) \leqq \langle (n_2-1)/2 \rangle$

とする．ここに，〈X〉は X を超えない最大の整数を表す．C_jの要素のうち，Eの影響を受けるものは高々，t（≦〈$(n_2-1)/2$〉）個であり，Eの影響を受けないものの方が多い．

以上により，次の定理が成立する．

［定理７．７］ 式(7.5)で表される巡回ＳＴ－ＡＮ符号において，受信語Vの各類C_jの要素間の多数決を取ることにより〈$(n_2-1)/2$〉重以下のすべての算術誤りEに対して符号整数Nを正しく復号できる．（証明略）

式(7.5)で示したＥＥ型巡回ＳＴ－ＡＮ符号に対して，定理７．６，７．７に基づく次の１段多数決論理復号の手順が適用できる．

《復号手順７．５》

Ⅰ． 受信語VのST表現におけるブロック N_i,(i=0,1,･･･,n_2-1) の中で，n_1けたすべてが "$\bar{1}$" のブロックがあれば，そのn_1けたすべてを "1" に置き換える．

Ⅱ． Ⅰで修正されたVに対して，C_j,(j=0,1,･･･,n_1-1) のそれぞれの類のn_2この要素の多数決を取り，その結果をb_jとすると，符号語ANの情報整数Nは，

$$N = \sum_{j=0}^{n_1-1} b_j 3^j$$

により復号される．

このとき，

$W_{ST}(E) \leqq \langle (n_2-1)/2 \rangle$

なる算術誤りに対して訂正可能である．このような１段多数決論理復号が適用できるその他の巡回ＳＴ－ＡＮ符号のクラスを表７．４に示す．

７．５．２　２段多数決論理復号

符号長，生成数，および，その符号語数がそれぞれ，

$$n = 2n_1n_2,\ A = (3^n-1)/(3^{n_1}-1)(3^{n_2}-1),$$

$$B = (3^{n_1}-1)(3^{n_2}-1),\ (n_1, n_2\ ;\text{正の奇数}) \qquad (7.8)$$

で与えられるＨＨ型巡回ＳＴ－ＡＮ符号を考える．

受信語Vに$(3^{n_2}-1)$を掛けると，

$$V(3^{n_2}-1) = AN(3^{n_2}-1) + E(3^{n_2}-1)$$

$$= A_1N + E(3^{n_2}-1)$$

ここに，$A_1=(3^n-1)/(3^{n_1}-1)$ である．上式に対して，法ABに関する絶対最小剰余をとると，

$$V(3^{n_2}-1) \bmod AB = (A_1N \bmod AB + E_1) \bmod AB \qquad (7.9)$$

ここに，$E_1=E(3^{n_2}-1) \bmod AB$ である．さらに，$A_1N \bmod AB = A_1N_1$ と表すことができる．このとき，A_1N_1は A_1で生成される符号長n のＥＥ型巡回ＳＴ－ＡＮ符号と考えられる．式(7.9)は符号語A_1N_1に算術誤りE_1を生じた受信語

$$V_1 = A_1N_1 + E_1$$

の法ABに関する絶対最小剰余である．したがって，

$$W_{ST}(E_1) \leqq W_{ST}(E(3^{n_2}-1)) \leqq 2W_{ST}(E)$$

であり，また，

$$A_1N_1 = (3^{(2n_2-1)n_1} + 3^{(2n_2-2)n_1} + \cdots + 3^{n_1} + 1)\ N_1$$

と表されることにより，

$$2W_{ST}(E) \leqq \lfloor (2n_2-1)/2 \rfloor \qquad (7.10)$$

ならば，前節の復号手順７．５によりを正しく復号できる．これにより，A_1N_1を復元できる．また，式(7.9)により，

$$E_1 \equiv V(3^{n_2}-1) - A_1N_1 \pmod{AB}$$

であるから，

$$E_1 = (V(3^{n_2}-1) \bmod AB - A_1N_1) \bmod AB$$

から，E_1が算出できる．

次に，$E(3^{n_2}-1)$を

$$E(3^{n_2}-1) = q \times AB + r, (r=E_1)$$

とおくと，

$$E = A_2 q + E_1/(3^{n_2}-1), (A_2=(3^n-1)/(3^{n_2}-1))$$

と表すことができ，

$$E_1/(3^{n_2}-1) \bmod AB = (A_2(q) \bmod AB + E) \bmod AB \qquad (7.11)$$

である．また，

$$A_2(-q) = q' \times AB + r', (r' = A_2(-q) \bmod AB)$$

とおくと，$A_2(q) \bmod AB = A_2N_2$ と表すことができる．このとき，A_2N_2 はA_2で生成される符号長n のＥＥ型巡回ＳＴ－ＡＮ符号語と考えられる．このため，式(7.11)は符号語A_2N_2 に算術誤りE を生じた受信語

$$V_2 = A_2N_2 + E$$

の法ABに関する絶対最小剰余であって，

$$A_2N_2 = (3^{(2n_1-1)n_2} + 3^{(2n_1-2)n_2} + \cdots + 3^{n_2} + 1) N_2$$

と表されることにより，

$$W_{ST}(E) \leqq \lfloor (2n_1-1)/2 \rfloor \qquad (7.12)$$

ならば，前節の復号手順７．５によりを正しく復号できる．これにより，A_2N_2を復元できる．また，式(7.10)により，

$$E = (V(3^{n_2}-1) \bmod AB - A_2N_2) \bmod AB$$

によりEが算出できる．以上により，

$$AN = R - E, N = (R-E)/A$$

から，N を正しく復号することができる．

以上により，次の定理が成立する．

［定理７．８］　式(7.8)で与えられる巡回ＳＴ－ＡＮ符号の任意の符号語ANは

$W_{ST}(E) \leqq \lfloor (2n_1-1)/2 \rfloor$

$2W_{ST}(E) \leqq \lfloor (2n_2-1)/2 \rfloor$

なるすべての算術誤りEに対して，２段の多数決論理復号により正しく復号される．

（証明略）

以上に基づく復号手順を以下に示す．

《復号手順７．６》

Ⅰ．　受信語V=AN+Eに対して，

$V(3^{n_2}-1) \bmod AB = A_1N_1 + E_1 \bmod AB$,

$(A_1 = (3^n-1)/(3^{n_1}-1),\ E_1 = E(3^{n_2}-1) \bmod AB)$

から，多数決論理復号により N_1を復号する．

Ⅱ．　N_1から，$A_1N_1 \rightarrow E_1 \rightarrow (E_1/(3^{n_2}-1)) \bmod AB$ を求める．そして，

$(E_1/(3^{n_2}-1)) \bmod AB = (A_2N_2 + E) \bmod AB$,

$(A_2 = (3^n-1)/(3^{n_2}-1))$

から，多数決論理復号により N_2を復号する．

Ⅲ．　N_2から，$A_2N_2 \rightarrow E$ を求める．

Ⅳ．　V－E を 生成数A で除算する．

このような２段多数決論理復号が適用できるその他の巡回ＳＴ－ＡＮ符号のクラスを表７．５に示す．

７．５．３　ｋ段多数決論理復号

前節に示した２段の多数決論理復号を一般のｋ(≧3)段の場合に拡張することによって，さらに多くの巡回ＳＴ－ＡＮ符号のクラスに対してこの原理に基づく復号方法を適用できる．

符号長，生成数，および，その符号語数がそれぞれ，

$$n = 2^{k-2} n_1 n_2 \cdots n_k,$$

$$A = (3^n-1)/(3^{n_1}-1)(3^{n_2}-1)\cdots(3^{n_k}-1),$$

$$B = (3^{n_1}\ 1)(3^{n_2}-1)\cdots(3^{n_k}-1),$$

$$(n_1, n_2 \cdots n_k ;\text{正の奇数}, k \geqq 3) \qquad (7.13)$$

で与えられる巡回ＳＴ－ＡＮ符号を考える．

受信語V=AN＋Eに対して，

$$V(3^{n_k}-1) \bmod AB$$

は，符号語A_1N_1に算術誤りE_1を生じた受信語$V_1 = A_1N_1 + E_1$の法ABに関する絶対最小剰余であると考えられる．ここに，

$$A_1 = (3^n-1)/(3^{n_1}-1)(3^{n_2}-1)\cdots(3^{n_{k-1}}-1),$$

$$A_1N_1 = A_1N \bmod AB,\ E_1 = E(3^{n_{k-1}}-1) \bmod AB$$

である．さらに，このV_1に対して，

$$V_1(3^{n_{k-1}}-1) \bmod AB$$

は，符号語A_2N_2に算術誤りE_2を生じた受信語$V_2 = A_2N_2 + E_2$の法ABに関する絶対最小剰余であると考えられる．ここに，

$$A_2 = A_1(3^{n_{k-1}}-1),$$

$$A_2N_2 = A_2N_1 \bmod AB,\ E_2 = E_1(3^{n_{k-1}}-1) \bmod AB$$

である．以下，同様にして，V_{k-1}まで繰り返せば，

$$A_{k-1} = A_{k-2}(3^{n_2}-1),$$

$$A_{k-1}N_{k-1} = A_{k-1}N_{k-2} \bmod AB,\ E_{k-1} = E_{k-2}(3^{n_2}-1) \bmod AB$$

を得る．ここで，

$$V_{k-1} = A_{k-1}N_{k-1} + E_{k-1}$$

とすれば，これは，A_{k-1}で生成されるＥＥ型巡回ＳＴ－ＡＮ符号の符号語$A_{k-1}N_{k-1}$に算術誤りE_{k-1}を生じた受信語であると考えられる．よって，

$$W_{ST}(E_{k-1}) \leqq 2W_{ST}(E_{k-2}) \leqq 2^2W_{ST}(E_{k-3}) \leqq \cdots$$

$$\cdots \leqq 2^{k-2}W_{ST}(E_1) \leqq 2^{k-1}W_{ST}(E)$$

により，

$$2^{k-1}W_{ST}(E) \leqq \lfloor (2^{k-2}n_2n_3\cdots n_k - 1)/2 \rfloor \qquad (7.14)$$

ならば，１段多数決論理復号（復号手順７．５）により，N_{k-1}を正しく復号することができる．これにより，$A_{k-1}N_{k-1}$ さらに E_{k-1}が求められる．

$E_{k-2}(3^{n_2}-1)$を

$$E_{k-2}(3^{n_2}-1) = q \times AB + r, \quad (r = E_{k-1}/(3^{n_2}-1) \bmod AB)$$

とおくと，

$$E_{k-2} = A'_{k-2}q + E_{k-1}/(3^{n_2}-1), \quad (A'_{k-2}=(3^n-1)/(3^{n_2}-1)$$

と表すことができ，

$$E_{k-1}/(3^{n_2}-1) \bmod AB = (A'_{k-2}(-q) \bmod AB + E_{k-2}) \bmod AB$$

である．また，

$$A'_{k-2}(q) = q' \times AB + r'$$

とおくと，$(A'_{k-2}(-q))\bmod AB = A'_{k-2}N'_{k-2}$ と表すことができる．このため，

$$V'_{k-2} = A'_{k-2}N'_{k-2} + E_{k-2}$$

とすると，これは，A'_{k-2} で生成されるＥＥ型巡回ＳＴ－ＡＮ符号の符号語 $A'_{k-2}N'_{k-2}$ に算術誤り E_{k-2} を生じた受信語と考えることができる．よって，

$$W_{ST}(E_{k-2}) \leqq 2^{k-2}W_{ST}(E)$$

から，

$$2^{k-2}W_{ST}(E) \leqq \lfloor (2^{k-2}n_1n_3n_4\cdots n_k - 1)/2 \rfloor$$

なら，多数決論理復号により N'_{k-2} を正しく復号することができる．これにより，$A'_{k-2}N'_{k-2}$ さらに E_{k-2} を得る．以下，同様にして，E_{k-3}，…，E_1を漸化的に得ることができる．そして最後に，

$$E(3^{n_k}-1) = q \times AB + r, \quad (r = E_1)$$

とおくと，これも同様にして，

$$E/(3^{n_k}-1) \bmod AB = (A'_{k-2}(-q) \bmod AB + E) \bmod AB$$
$$= (A'N' + E) \bmod AB$$
$$= V' \bmod AB$$

と表すことができる．したがって，

$$2^{k-2} W_{ST}(E) \leqq \lfloor (2^{k-2} n_1 n_2 \cdots n_{k-1} - 1)/2 \rfloor$$

なら，多数決論理復号によりN'を正しく復号できる．これにより，A'N' を得る．よって，

$$E = (V' \bmod AB + A'N') \bmod AB$$
$$AN = V - E,\ N = (V - E)/A$$

から，Nを正しく復号することができる．

以上により，次の定理が成立する．

［定理７．９］ 式(7.13)で与えられる巡回ＳＴ－ＡＮ符号の任意の符号語ANは

$$W_{ST}(E) \leqq \lfloor (2^{k-2} n'_k - 1)/2 \rfloor ,$$

$$2W_{ST}(E) \leqq \lfloor (2^{k-2} n'_{k-1} - 1)/2 \rfloor ,$$

……

$$2W_{ST}(E) \leqq \lfloor (2^{k-2} n'_1 - 1)/2 \rfloor , \quad (n_i = n_1 n_2 \cdots n_k / n_i)$$

なるすべての算術誤りEに対して，ｋ段の多数決論理復号により正しく復号される．

（証明略）

以上に基づく復号手順を以下に示す．

《復号手順７．７》

Ｉ． 受信語V=AN+Eに対して，

$V_{k-1} \bmod AB = (A_{k-1} N_{k-1} + E_{k-1}) \bmod AB$

から，N_{k-1} を復号手順７．５により復号する．

Ⅱ．上のN_{k-1}から，$E_{k-1} = (V_{k-1} \bmod AB - A_{k-1}N_{k-1}) \bmod AB$ を求め，

$V'_{k-2} \bmod AB = (E_{k-2}/(3^{n_2}-1)) \bmod AB$

$= (A'_{k-2}N'_{k-2} + E_{k-2}) \bmod AB$, $(A'_{k-2}=(3^{n}-1)/(3^{n_2}-1))$

から，N'_{k-2} を復号する．

Ⅲ．上のN'_{k-2}から，Ⅱと同様にして，$N'_{k-3}\cdots N'_1$ を順次漸化的に復号する．

Ⅳ．N'_1 から，$E_1 = (V'_1 \bmod AB - A'_1N'_1) \bmod AB$ を求め，

$V' \bmod AB = (E_1/(3^{n_k}-1)) \bmod AB$

$= (A'N' + E) \bmod AB$, $(A'=(3^{n}-1)/(3^{n_k}-1))$

から，N'を復号する．このN'から，

$E = (V' \bmod AB - A'N') \bmod AB$

を得る．

Ⅴ．V－E を 生成数A で除算する．

このようなｋ段多数決論理復号が適用できるその他の巡回ＳＴ－ＡＮ符号として，次の形の符号がある．

$n = 2^{k-2}n_1n_2\cdots n_k$,

$A = 2^j(3^n-1)/(3^{n_1}-1)(3^{n_2}-1)\cdots(3^{n_k}-1)$,

$B = (3^{n_1}-1)(3^{n_2}-1)\cdots(3^{n_k}-1)/2^j$,

($n_1, n_2\cdots n_k$；正の奇数，$k \geqq 3$)　　(7.15)

７．６　結　言

第３章から６章までに述べたＳＴ－ＡＮ符号のそれぞれに対して，誤り訂正の原理とそれらに基づく復号手順を示した．

一般のＳＴ－ＡＮ符号の復号に関しては，誤りとそのシンドローム対応表によ

るものと，この表を必要としないものを示した．後者は，その手順がいたって簡単であり，表を記憶するためのメモリを必要としない．

巡回ＳＴ－ＡＮ符号に関しては，まず，エラー・トラッピングによる復号方法２つを示した．これらは，受信語の巡回けた移動を利用するものである．ひとつは，単純エラー・トラッピング復号といい，基本的で簡明な手順となる．あるt(≧2)重誤り訂正可能な巡回ＳＴ－ＡＮ符号に対しては，検査窓による窓付きエラー・トラッピング復号を開発した．単純エラー・トラッピングで訂正できない正当なt重誤りも，この復号方法によれば，訂正できることを確かめた．個々の巡回ＳＴ－ＡＮ符号の復号方法を検討する際，窓を必要とするか否か，必要とするならどの位置に窓を設けるかという問題がある．これに対しては，簡便で組織的な一方法を示した．この方法を用いて，復号手順７．２（検査窓１個）で正当な誤りのすべてを訂正できる符号と窓の位置を例示した．

前節においては，多数決論理復号を示した．そこでは，１段，２段，さらにこれを一般のｋ段の場合に拡張し，代表的な符号に対してそれぞれの復号手順を示し，また，このような復号方法が適用可能な巡回ＳＴ－ＡＮ符号のクラスを示した．

負巡回ＳＴ－ＡＮ符号の復号方法では，その構造から，巡回ＳＴ－ＡＮ符号のエラー・トラッピング復号手順に類した負巡回けた移動によるものを示した．

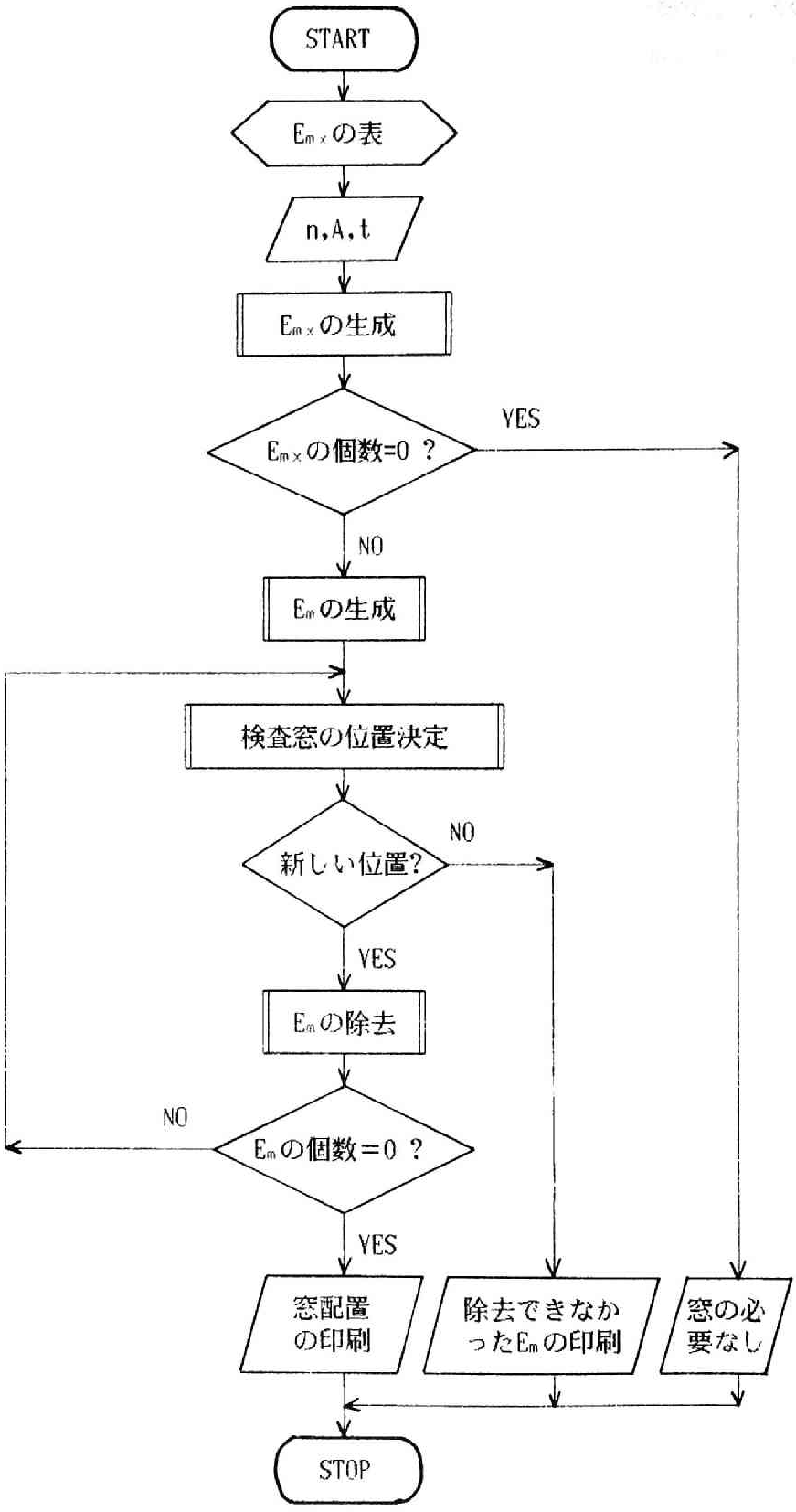

図７．１　検査窓の配置の手順

表7.1　正当な誤り（E）とシンドローム（S(E)）の対応表

S(E)	E	S(E)	E
1	1	47	240
2	2	48	-2268
3	3	49	242
4	4	50	243
6	6	51	244
7	972	52	-720
8	8	53	246
9	9	54	54
10	10	55	55
12	12	59	59
14	1944	61	2184
16	-756	62	-324
17	-2106	63	2186
18	18	64	2187
21	2916	65	2188
23	216	67	2190
24	24	69	648
26	26	70	-702
27	27	72	72
28	28	73	73
30	30	77	77
31	-162	78	78
34	-738	79	-2430
36	36	80	80
37	2160	81	81
38	810	82	82
40	-732	84	84
41	234	85	-108
42	-730	86	-1458
43	-729	90	90
44	-728	91	2214
46	-726	93	-486

表7.2　t重誤りの絶対最小巡回シフトの最大値E_{mx}とそのパターン

t	r	E_{mx}
1	0	X
2	0	XX
	1	0XX
3	0	XXX
	1	0XXX
	2	0X0XX
4	0	XXXX
	1	0XXXX
	2	0XX0XX
	3	0X0X0XX
5	0	XXXXX
	1	0XXXXX
	2	0XX0XXX
	3	0X0XX0XX
	4	0X0X0X0XX
6	0	XXXXXX
	1	0XXXXXX
	2	0XXX0XXX
	3	0XX0XX0XX
	4	0X0XX0X0XX
	5	0X0X0X0X0XX
7	0	XXXXXXX
	1	0XXXXXXX
	2	0XXX0XXXX
	3	0XX0XX0XXX
	4	0X0XX0XX0XX
	5	0X0X0XX0X0XX
	6	0X0X0X0X0X0XX
8	0	XXXXXXXX
	1	0XXXXXXXX
	2	0XXXX0XXXX
	3	0XX0XXX0XXX
	4	0XX0XX0XX0XX
	5	0X0XX0X0XX0XX
	6	0X0X0XX0X0X0XX
	7	0X0X0X0X0X0X0XX

$n=qt+r$, $(0 \leqq r < q)$, $X=(00\cdots01)_{ST}$.
$(q-1)$個

表7.2　t重誤りの絶対最小巡回シフトの最大値E_{mx}とそのパターン（その2）

t	r	E_{mx}
9	0	XXXXXXXXX
	1	0XXXXXXXXX
	2	0XXXX0XXXX
	3	0XXX0XXX0XX
	4	0XX0XX0XX0XX
	5	0X0XX0XX0XX0X
	6	0X0XX0X0XX0X0XX
	7	0X0X0X0XX0X0X0XX
	8	0X0X0X0X0X0X0X0XX
10	0	XXXXXXXXXX
	1	0XXXXXXXXX
	2	0XXXXX0XXXX
	3	0XXX0XXX0XXX
	4	0XX0XXX0XX0XX
	5	0XX0XX0XX0XX0XX
	6	0X0XX0XX0X0XX0XX
	7	0X0X0XX0X0XX0X0XX
	8	0X0X0X0XX0X0X0X0XX
	9	0X0X0X0X0X0X0X0X0XX

表７．３　検査窓を必要とする巡回ＳＴ－ＡＮ符号の例

符号長;n	符号語数; B	生成数;A	誤り訂正能力; t	$\|E_m\| > A/2$ を満たすE_mの個数	窓の位置; k
11	46	3851	3	2^3	7
12	65	8176	3	2^3	8
15	143	100342	3	2^3	10
16	68	633040	4	2^4	12
16	85	506432	4	2^4	12
16	544	79130	3	2×2^3	10
16	680	63304	3	2×2^3	10
16	697	61760	3	2×2^3	10
16	965	44608	3	2×2^3	10
16	1088	39565	3	4×2^3	10
18	481	805448	4	$21\times2^4+2^3$	13
20	440	7924510	4	10×2^4	15
20	550	6339608	4	10×2^4	15
20	275	12679216	5	$31\times2^5+2^4$	16
22	3082	10182044	4	27×2^4	16
22	6164	5091022	4	$63\times2^4+2\times2^3$	16
24	1435	196815008	5	$203\times2^5+10\times2^4$	19
24	2665	105977312	5	$232\times2^5+10\times2^4$	19
25	8951	94658542	4	35×2^4	18

表７．４　１段多数決論理復号（復号手順７．５を応用したもの）可能な巡回ＳＴ－ＡＮ符号

符号長;n	生成数;A	符号語数;B	備考
$2n_1n_2$	$(3^n-1)/(2^j(3^{n_1}-1))$	$2^j(3^{n_1}-1)$	j=1,2
n_1n_2	$2(3^n-1)/(3^{n_1}-1)$	$(3^{n_1}-1)/2$	
$2n_1n_2$	$(3^n-1)/(3^{n_1}+1)$	$(3^{n_1}+1)$	
$2n_1n_2$	$(3^n-1)/(2(3^{n_1}+1))$	$2(3^{n_1}+1)$	
$2n_1n_2$	$2^j(3^n-1)/(3^{n_1}+1))$	$(3^{n_1}+1)/2^j$	j=1,2
$2^kn_1n_2$	$(3^n-1)/(3^{2^kn_1}-1)$	$(3^{2^kn_1}-1)$	
$2^kn_1n_2$	$2^j(3^n-1)/(3^{2^kn_1}-1)$	$(3^{2^kn_1}-1)/2^j$	j=1,2
$2^{k+1}n_1n_2$	$(3^n-1)/(3^{2^kn_1}+1)$	$(3^{2^kn_1}+1)$	
$2^{k+1}n_1n_2$	$(3^n-1)/(2^j(3^{2^kn_1}+1))$	$2^j(3^{2^kn_1}+1)$	j=1,2,…,k+2

表7.5　2段多数決論理復号（復号手順7.6を応用したもの）可能な巡回ＳＴ－ＡＮ符号

符号長;n	生成数;A	符号語数;B	備考
$2n_1n_2$	$(3^n-1)/(2(3^{n_1}-1)(3^{n_2}-1))$	$2(3^{n_1}-1)(3^{n_2}-1)$	
n_1n_2	$2^j(3^n-1)/((3^{n_1}-1)(3^{n_2}-1))$	$(3^{n_1}-1)(3^{n_2}-1)/2^j$	j=1,2
$2^{k+1}n_1n_2$	$(3^n-1)/((3^{2^k n_1}-1)(3^{n_2}-1))$	$(3^{2^k n_1}-1)(3^{n_2}-1)$	
$2^kn_1n_2$	$2^j(3^n-1)/((3^{2^k n_1}-1)(3^{n_2}-1))$	$(3^{2^k n_1}-1)(3^{n_2}-1)/2^j$	j=1,2,…,k+3
$4n_1n_2$	$(3^n-1)/((3^{n_1}+1)(3^{n_2}+1))$	$(3^{n_1}+1)(3^{n_2}+1)$	
$2n_1n_2$	$2^j(3^n-1)/((3^{n_1}+1)(3^{n_2}+1))$	$(3^{n_1}+1)(3^{n_2}+1)/2^j$	j=1,2
$2^{k+1}n_1n_2$	$(3^n-1)/((3^{2^k n_1}+1)(3^{n_2}+1))$	$(3^{2^k n_1}+1)(3^{n_2}+1)$	
$2^{k+1}n_1n_2$	$(3^n-1)/(2^j(3^{2^k n_1}+1)(3^{n_2}+1))$	$2^j(3^{2^k n_1}+1)(3^{n_2}+1)$	j=1,2,…,k
$2n_1n_2$	$(3^n-1)/((3^{n_1}-1)(3^{n_2}+1))$	$(3^{n_1}-1)(3^{n_2}+1)$	
$2n_1n_2$	$2^j(3^n-1)/((3^{n_1}-1)(3^{n_2}+1))$	$(3^{n_1}-1)(3^{n_2}+1)/2^j$	j=1,2,3
$2^{k+2}n_1n_2$	$(3^n-1)/((3^{2^k n_1}-1)(3^{n_2}+1))$	$(3^{2^k n_1}-1)(3^{n_2}+1)$	
$2^{k+2-j}n_1n_2$	$2^j(3^n-1)/((3^{2^k n_1}-1)(3^{n_2}+1))$	$(3^{2^k n_1}-1)(3^{n_2}+1)/2^j$	j=1,2
$2^{k+1}n_1n_2$	$(3^n-1)/((3^{2^k n_1}+1)(3^{n_2}-1))$	$(3^{2^k n_1}+1)(3^{n_2}-1)$	
$2^{k+1}n_1n_2$	$(3^n-1)/(2^j(3^{2^k n_1}+1)(3^{n_2}-1))$	$2^j(3^{2^k n_1}+1)(3^{n_2}-1)$	j=1,2,…,k

第８章　結　論

緒論でも述べたように３進独特の対称３進表現（ＳＴ表現）を用いる種々の３値ディジタルシステムが開発され，それらの信頼性を向上させることは重要な問題のひとつと考えられる．本論文は，このようなシステムの大きな特長のひとつである算術演算における誤り検出訂正符号を提案した．この符号は，ＳＴ－ＡＮ符号といい，２進算術ＡＮ符号を対称３進符号に拡張したものである．２進符号と同様，この符号もまた．演算装置のみならずディジタルデータ伝送路や記憶装置を含むディジタルシステムにも有効である．

第２章では，この符号に導入されるST算術重みとST算術距離を定義し，これらの基本的な性質を明らかにした．この算術重みや算術距離は，リー距離の考え方によるものであり，これらは３値ディジタルシステムにおける基本回路の主な構成方式のひとつである３レベル信号方式に対してはハミング距離の考え方による従来の算術距離より合理的である．

第３章では．ST算術距離を導入したＳＴ－ＡＮ符号を定義し，その基礎理論を述べた．最小距離が４以下の代表的なＳＴ－ＡＮ符号を構成するため．生成数 A からその符号語数を与える公式を導いた．また，最小距離が５以上の場合は．電子計算機を用いて調査した．以上により，これらの代表的な符号を得た．

第４章では．巡回ＳＴ－ＡＮ符号を定義し，その基礎理論を述べた．これに基づいて，第５章では，符号語数 B で規定される巡回ＳＴ－ＡＮ符号の構成方法を示した．このような符号の整数論的構造に基づき，最小距離を具体的に算定する方法を示し，種々の B に対して規定される符号の最小距離の算定公式を導いた．これらの公式により得られる符号の最小距離は大きく，多重誤り訂正可能な符号である．なお，最小距離が４以下の符号の構成には，第３章の公式のいくつかを利用できる．

第６章では．巡回ＳＴ－ＡＮ符号とその構造が類似した負巡回ＳＴ－ＡＮ符号を定義した．この符号の構成方法，最小距離の算定においては，全く並行した議論の展開が可能である．

第７章では，以上述べたＳＴ－ＡＮ符号の誤り訂正の原理とそれに基づく復号

方法を提案した．一般のＳＴ－ＡＮ符号の復号方法として，シンドロームを用いる単純計算の繰り返しによる方法を示した．巡回ＳＴ－ＡＮ符号の復号方法として，エラー・トラッピングによるものと多数決論理に基づくものを示した．後者の誤り訂正の原理が適用できる符号は限定されるが，復号における個々の操作は簡潔である．負巡回ＳＴ－ＡＮ符号の復号方法としては，巡回ＳＴ－ＡＮ符号のエラー・トラッピングに類似のものが適用できる．いずれの場合も，算術誤りの値が正負にかかわらず統一的に処理できるため，これらの復号手順は簡明である．また，個々の操作においても算術的な処理が多く含まれており，ST表現の算術演算にもつ特長を生かすことができると考えられる．

本論文で述べたＳＴ－ＡＮ符号は，ランダム誤りの検出訂正に有効である．伝送路や演算装置においては，雑音や装置の故障などの障害によって連続する数けたに誤りが発生する場合が考えられる．このようなバースト誤り[7][45]に対しても研究を進める方針である．また，ＳＴ－ＡＮ符号を算術距離も含めて，さらに一般のｒ進符号へ拡張していくことを考えている．とくに，ｒが奇数の対称奇ｒ進算術ＡＮ符号[46]，次いで，ｒが偶数の場合，4,8,16 などの 2^a 進算術ＡＮ符号へ研究を進めていく方針である．

謝　　辞

本研究を行うにあたり，御懇切なる御指導，御鞭撻を賜った京都大学工学部数理工学科 長谷川利治教授に心より感謝の意を表します．

研究の全過程を通じ，直接御指導，御教示をいただいた徳島大学工学部情報工学科 島田良作教授に深く感謝の意を表します．また，有益なる御討論と御助言をいただいた山本米雄助教授，青江順一助手に感謝いたします．さらに，石田富士雄技官，堀江康雄氏（現在，松下電器産業㈱），大学院生 村上龍太郎氏には熱心な討論ならびに種々な面で御協力いただき，ここに厚くお礼申します．

本研究の当初において貴重な多くの文献を快くお送りいただき，また，有益なる御討論を賜った岐阜大学工学部電子工学科 後藤宗弘教授に深く感謝いたします．

激励のお言葉をいただいた徳島文理大学 黒田嘉一郎学長，同短期大学部 保科千代次部長，商科 福本憲一科長，薬学部 川西勝信教授（元商科科長），くわえて御助言をいただいた薬学部 大崎中男教授（一般教養数学担当）に深く感謝します．また，計算機の操作等種々の面でお世話いただいた森田教子助手をはじめ商科研究室の諸氏には厚くお礼申します．

参　考　文　献

[1] Avizienis, A ; "Arithmetic error codes : cost and effectiveness studies for application in digital system design", IEEE Trans. on Computers, C-20, 11, pp.1322-1331,(1971)

[2] Berlekamp, E.R. ; "Algebraic Coding Theory", McGraw Hill, New York, (1968)

[3] Brown, D.T. ; "Error detecting and correcting binary codes for arithmetic operations", IRE Trans., EC-9, pp.333-337,(1960)

[4] Chen, C.H. ; "An algebraic model of arithmetic codes", IEEE Trans. on Computers, C-31, 4, pp.318-321,(1982)

[5] Chen, C.L., Chien, R.T. and Chao-Kailiu ; "On majority logic decodable arithmetic codes", IEEE Trans., Inf. Theory, IT-19, pp.678-682,(1973)

[6] Chiang, C.L. and Reed, I.S. ; "Arithmetic norms and bounds of the arithmetic AN codes", IEEE Trans. Inf. Theory, IT-16, pp.470-476, (1970)

[7] Chien R.T. ; "On linear residue codes for burst-error correction", IEEE Trans. Inf. Theory, IT-10, pp.127-133,(1964)

[8] Dao, T.T.; "Complex number arithmetic with balanced ternary logic", Proc. of The 9th Int. Symp. on Multiple-Valued Logic, pp.281-289, (1979)

[9] Diamond, J.M.; "Checking for digital computers", Proc. IRE, 43, pp. 487-488, 4,(1955)

[10] Ecker, A. ; "How to compute the minimum distance for cyclic AN codes over an arbitrary base", Inf. and Control, 46, pp219-240, (1980)

[11] Erosh, I.L. and Erosh, E.L. ; "Arithmetic codes with correction of multiple errors", Problemy Predaci Informacii, 3, 4, pp.72-80, (1967)

[12] 福村，後藤 ："算術符号理論"，コロナ社，東京,(1978)

[13] Garner, H.L. ; "Error codes for arithmetic operations", IEEE Trans. on Electric Computers, EC-15, 5, pp.763-770,(1966)

[14] 後藤 ："対称３進表現と３値ミニマル表現"，昭和５６年度電子通信学会情報システム部門全国大会分冊１，pp.4.(Oct.1981)

[15] 後藤 ："巡回ＳＴＡＮ符号の距離に関する考察"，信学論(A)，J65-D，11，pp.1115-1120.(1982)

[16] Goto, M. ; "Perfect and near perfect AN codes in symmetric multivalued number representation", 第６回情報理論とその応用研究会，pp.222-226,(Nov. 1983)

[17] Hamming, R.W. ; "Error detecting and error correcting codes", Bell System Tech. J., Vol.129, pp.147-160,(1950)

[18] Hartman, W.F.; "Arithmetic codes", Univ.of Notre Dame, Disertation for the Degree of Doctor of Philosophy, Notre Dame, Indiana,(1975)

[19] Higuchi, T. and Hoshi, H. ; "Special-purpose ternary computer for digital filtering", Proc. of The 8th Int. Symp. on Multiple-valued Logic, pp.47-54,(May. 1978)

[20] Hwang, T. and Hartmann, C.R.P. ; "Some results on arithmetic codes of composite length", IEEE Trans. Inf. Theory, IT-24, pp.94-99, (1978)

[21] Kasami, T. ; "A decoding procedure for multiple error-correcting codes", IEEE Trans. Inf. Theory, IT-10, pp.134-139,(1964)

[22] Lee, C.Y. ; "Some properties of nonbinary error-correcting codes", IRE Trans, IT-4, pp.77-82,(1958)

[23] Mandelbaum, D. ; "Arithmetic codes with large distance", IEEE Trans. Inf. Theory, IT-13, pp.237-242,(1967)

[24] Massey, J.L. ; "Survey of residue coding for arithmetic errors", International Computration Center Bulleten, 3,pp.195-209,(1963)

[25] 三根, 長谷川, 池田, 新谷 ; "三値論理回路の一構成", 信学論(C), 51-C, 12, pp.573-580,(1968)

[26] 三根, 長谷川, 島田, "三進四則演算方式について", 信学論(C), 54-C, 1, pp.66-73,(1971)

[27] 三根,長谷川,島田 ; "三進算術演算装置", 情報処理, 12, 9, pp.528-533, (1971)

[28] 牟田征一 ; "一対のトランジスタを用いた３値基本回路", 信学論 (C), 52-C, pp.574-575,(1969)

[29] Morris, D.J. and Alexander, W. ; "An introduction to the ternary code number systems", Elect.Engeneering, 32, 392, pp.554-557,(Sept. 1960)

[30] Neumann, P.G. and Rao, T.R.N ; "Error-correcting codes for byte-organized arithmetic processors", IEEE Trans. on Computers, C-24, 3, pp.226-232,(1975)

[31] Ohkura, Y., Shimada, R. and Hasegawa, T. ; "Symmetric ternary arithmetic weight and symmetric ternary arithmetic AN codes", Proc. of The 11th Int. Symp. on Multiple-Valued Logic, pp.163-167,(May. 1981)

[32] 大倉,島田,長谷川 ; "対称三進算術ＡＮ符号", 信学論(D), J64-D, 6, pp. 66-73,(1981)

[33] 大倉,島田,長谷川 ; "巡回ＳＴ－ＡＮ符号について", 信学論(D), J65-D, 11, pp.1358-1365,(1982)

[34] Ohkura, Y., Shimada, R. and Hasegawa, T. ; "Cyclic ST-AN codes and modular ST distance", Proc. of The 13th Int. Symp. on Multiple-Valued Logic, pp.294-299,(May. 1983)

[35] 大倉,島田,長谷川 ; "巡回ＳＴ－ＡＮ符号のエラー・トラッピング復号", 第６回情報理論とその応用研究会, pp.298-303,(1983)

[36] Peterson, W.W. and Weldon, E.J.Jr ： "Error-Correcting Codes", 2nd ed. M.I.T. Press, Cambridge, Mass.,(1972)

[37] Rao, T.R.N. and Trchan, A.K. ： "Single error correcting nonbinary arithmetic codes", IEEE Trans., Inf. Theory, IT-16, pp.604-608, (1970)

[38] Rao, T.R.N. and Garcia, O.N. ： "Cyclic and multiresidure codes for arithmetic operations", IEEE Trans. Inf. Theory, IT-17, pp.85-91, (1971)

[39] Rao, T.R.N. ： "Error Coding for Arithmetic Processors", Academic Press, New York,(1974)

[40] 島田,山本,青江,大倉,堀江 ： "ＨＨ型巡回ＳＴ－ＡＮ符号", 信学論(D), J66-D, 12, pp.1339-1346,(1983)

[41] 島田, 大倉, 村上 ："多数決論理復号可能な巡回ＳＴ－ＡＮ符号", 信学論(D), J68-D, 6, pp.1218-1225,(1985)

[42] 田山, 舛田, 佐藤 ："対称３値論理系の提案", 信学論(D), J59-D, 4, pp. 245-251,(1976)

[43] Tsao-Wu, N. ："Arithmetic cyclic codes", Notheastern Univ., Boston, Mass., Part I of Communication Theory Group Report, No.10,(1968)

[44] ヴィノグラードフ著, 三瓶,中山共訳 ： "整数論入門", 共立全書 517, 共立出版, 東京,(1977)

[45] 島田, 大倉, 村上 ："バースト訂正可能な巡回ＳＴ－ＡＮ符号（仮題）", 信学論(D), 投稿中

[46] Shimada, R., Ohkura, Y. and Aoe, I ："Nonbinary arithmetic AN codes using odd radix expressions", IEEE Trans. on Computers, C-34, 11, pp.1050-1056,(1985)